Product Guide

Revision C

McAfee Advanced Threat Defense 3.4.8

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

This guide provides the information you need to work with your McAfee product.

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
ℹ	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
❗	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1 Go to the **Knowledge Center** tab of the McAfee ServicePortal at http://support.mcafee.com.

2 In the **Knowledge Base** pane, click a content source:

- **Product Documentation** to find user documentation
- **Technical Articles** to find KnowledgeBase articles

3 Select **Do not clear my filters**.

4 Enter a product, select a version, then click **Search** to display a list of documents.

1

Malware detection and McAfee® Advanced Threat Defense

Over the years, malware has evolved into a sophisticated tool for malicious activities such as stealing valuable information, accessing your computer resources without your knowledge, and for disrupting business operations. At the same time, technological advancement provides limitless options to deliver malicious files to unsuspecting users. Hundreds of thousands of new malware variants every day make the job of malware detection even more complex. Traditional anti-malware techniques are no longer sufficient to protect your network.

McAfee's response to this challenge is the Advanced Threat Defense solution. This is an on-premise Appliance that facilitates detection and prevention of malware. Advanced Threat Defense provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.

Advanced Threat Defense has the added advantage of being an integrated solution. In addition to its own multi-level threat detection capabilities, its ability to seamlessly integrate with other McAfee security products, protects your network against malware and other Advanced Persistent Threats (APTs).

Contents

The malware threat scenario

Any software capable of being involved in hostile activities with respect to a computer, application, or network can be termed as malware. Advanced Threat Defense is designed for detecting file-based malware.

Earlier, users received malware as attachments in their emails. With the upsurge in Internet applications, users only need to click a link to download files. Today, there are many other options to post such files — blogs, social networking sites, web sites, chat messages, web mails, message boards, and so on. The key challenges in tackling this issue are to detect malware in the shortest possible time and also contain it from spreading to other computers.

There are four major aspects to an anti-malware strategy:

- Detection of file downloads: When a user attempts to download a file from an external resource, your security product must be able to detect it.
- Analysis of the file for malware: You must be able to verify if the file contains any known malware.

- Block future downloads of the same file: Subsequently, if the file is found to be malicious, your anti-malware protection must prevent future downloads of the same file or its variants.
- Identify and remediate affected hosts: Your security system must be able to identify the host which executed the malware, and also detect the hosts to which it has spread. Then, it must provide an option to quarantine the affected hosts until they are clean again.

The Advanced Threat Defense solution

A security solution that relies on a single method or process might not be adequate to provide complete and reliable protection from malware attacks. You might need a multi-layered solution that involves various techniques and products. The solution can include pattern matching, global reputation, program emulation, static analysis, and dynamic analysis. All these layers must be seamlessly integrated and provide you with a single point of control for easy configuration and management. For example, pattern matching might not detect zero-day attacks. Similarly, static analysis takes less time than dynamic analysis. However, malware can avoid static analysis by code obfuscation. Malware can escape dynamic analysis too by delaying execution or take an alternate execution path if the malware detects that it is being run in a sandbox environment. This is why a reliable protection from malware requires a multi-level approach.

There are other industry-leading McAfee anti-malware products for the web, network, and endpoints. However, McAfee recognizes that a robust anti-malware solution requires a multi-layered approach, the result of which is Advanced Threat Defense.

The Advanced Threat Defense solution primarily consists of the Advanced Threat Defense Appliance and the pre-installed software. The Advanced Threat Defense Appliance is available in two models. The standard model is the ATD-3000. The high-end model is the ATD-6000.

Advanced Threat Defense integrates its native capabilities with other McAfee products to provide you a multilayered defense mechanism against malware:

- Its preliminary detection mechanism consists of a local blacklist to quickly detect known malware.
- It integrates with McAfee® Global Threat Intelligence™ (McAfee GTI) for cloud-lookups to detect malware that has already been identified by organizations throughout the globe.
- It has the McAfee Gateway Anti-Malware Engine embedded within it for emulation capability.

- It has the McAfee Anti-Malware Engine embedded within it for signature-based detection.
- It dynamically analyzes the file by executing it in a virtual sandbox environment. Based on how the file behaves, Advanced Threat Defense determines its malicious nature.

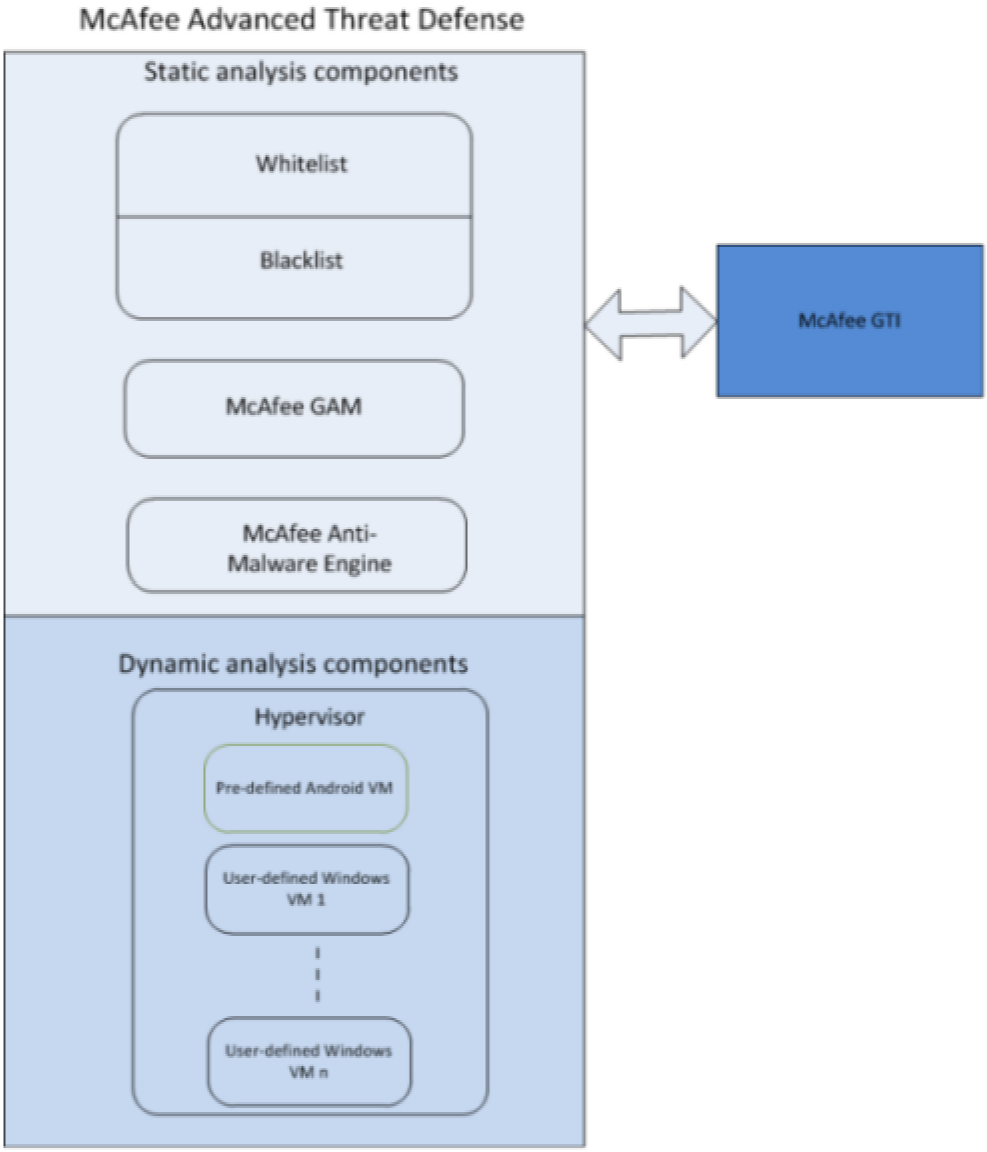

McAfee Advanced Threat Defense
Static analysis components
Whitelist
Blacklist
McAfee GAM
McAfee Anti-Malware Engine
McAfee GTI
Dynamic analysis components
Hypervisor
Pre-defined Android VM
User-defined Windows VM 1
User-defined Windows VM n

Figure 1-1 Components for malware analysis

McAfee Advanced Threat Defense deployment options

You can deploy McAfee Advanced Threat Defense in the following ways:

- Standalone deployment — This is a simple way of deploying McAfee Advanced Threat Defense. In this case, it is not integrated with other externally installed McAfee products. When deployed as a standalone Appliance, you can manually submit the suspicious files using the McAfee Advanced Threat Defense web application. Alternatively, you can submit the samples using an FTP client. This deployment option is used, for example, during the testing and evaluation phase, to fine-tune configuration, and to analyze suspicious files in an isolated network segment. Also, research engineers might use the standalone deployment option for detailed analysis of malware.

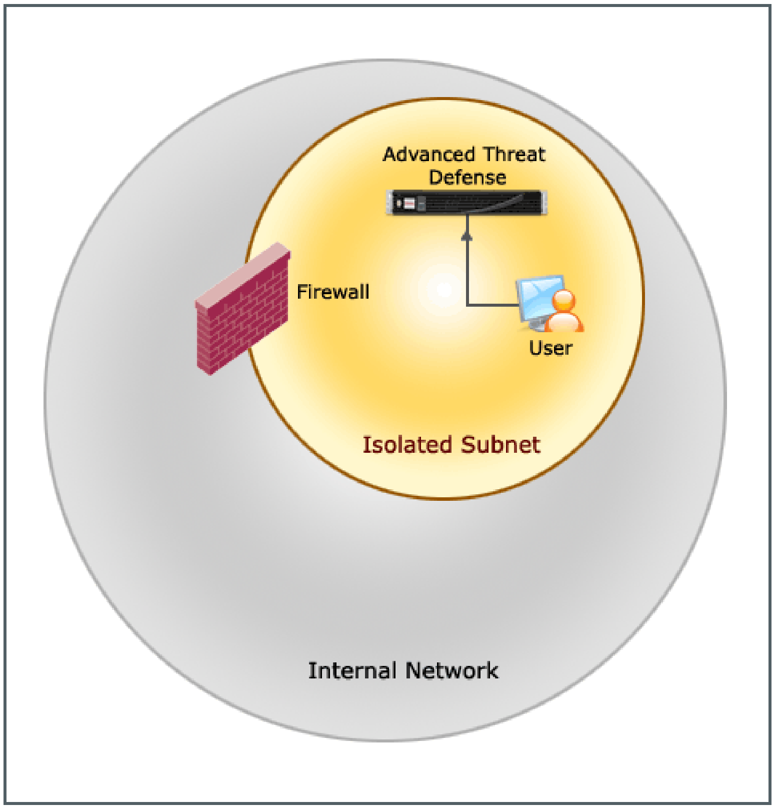


Figure 1-2 A standalone deployment scenario

- Integration with Network Security Platform — This deployment involves integrating McAfee Advanced Threat Defense with Network Security Platform Sensor and Manager.

  Based on how you have configured the corresponding Advanced Malware policy, an inline Sensor detects a file download and sends a copy of the file to McAfee Advanced Threat Defense for analysis. If McAfee Advanced Threat Defense detects a malware within a few seconds, the Sensor can block the download. The Manager displays the results of the analysis from McAfee Advanced Threat Defense.

  If McAfee Advanced Threat Defense requires more time for analysis, the Sensor allows the file to be downloaded. If McAfee Advanced Threat Defense detects a malware after the file has been downloaded, it informs Network Security Platform, and you can use the Sensor to quarantine the host until it is cleaned and remediated. You can configure the Manager to update all the Sensors about this malicious file. Therefore, if that file is downloaded again anywhere in your network, your Sensors might be able to block it.

  For information on how to integrate Network Security Platform and McAfee Advanced Threat Defense, refer to the latest *Network Security Platform Integration Guide.*

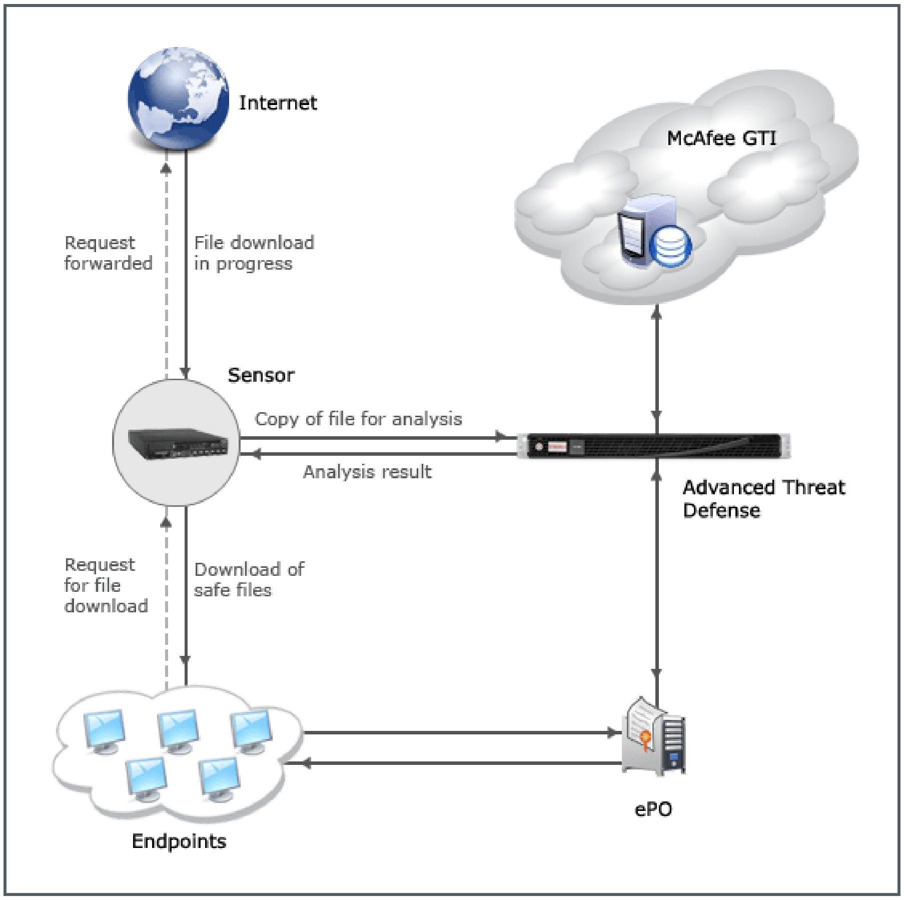


Figure 1-3 Integration with Network Security Platform and McAfee ePO

- Integration with McAfee® Web Gateway — You can configure McAfee Advanced Threat Defense as an additional engine for anti-malware protection. When your network user downloads a file, the native McAfee Gateway Anti-malware Engine on McAfee® Web Gateway scans the file and determines a malware score. Based on this score and the file type, McAfee® Web Gateway sends a copy of the file to McAfee Advanced Threat Defense for deeper inspection and dynamic analysis. A progress page informs your users that the requested file is being analyzed for malware. Based on the malware severity level reported by McAfee Advanced Threat Defense, McAfee® Web Gateway determines if the file is allowed or blocked. If it is blocked, the reasons are displayed for your users. You can view the details of the malware that was detected in the log file.

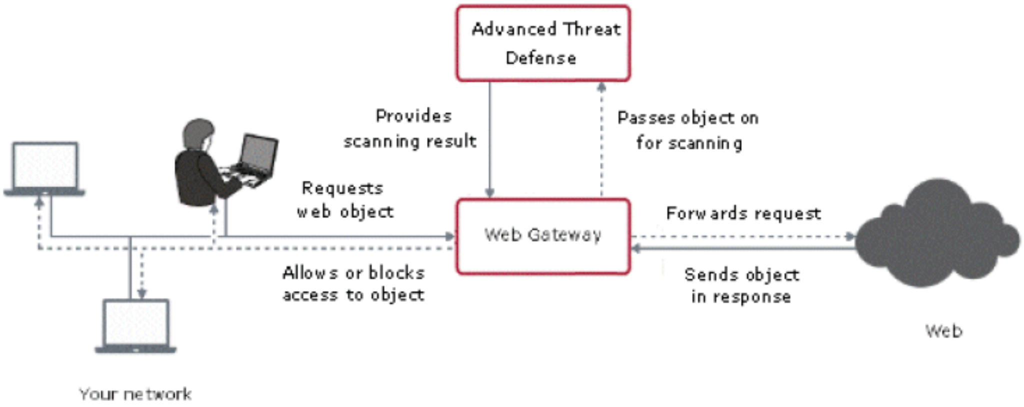


Figure 1-4 Integration with McAfee® Web Gateway

This design ensures that only those files that require an in-depth analysis are sent to McAfee Advanced Threat Defense. This balances your users' experience in terms of download speed and security. For information on how to integrate McAfee Advanced Threat Defense and McAfee® Web Gateway, see the *McAfee® Web Gateway Product Guide,* version 7.4.

- Integration with McAfee® ePolicy Orchestrator (McAfee ePO) — This integration enables McAfee Advanced Threat Defense to retrieve information regarding the target host. Knowing the operating system on the target host, enables it to select a similar virtual environment for dynamic analysis.

- Integration with McAfee® Next Generation Firewall (McAfee NGFW) — McAfee Next Generation Firewall integrates security features with high availability and manageability. It integrates application control, Intrusion Prevention System (IPS), and evasion prevention into a single, affordable solution. Following steps should be performed by McAfee Next Generation Firewall customer in order to integrate McAfee Next Generation Firewall with McAfee Advanced Threat Defense:

  1. Create a user called “ngfw” on Advanced Threat Defense after logging into Advanced Threat Defense as "admin". This user has the same privileges as the "nsp" user.

  2. Restart amas from the CLI.

  3. Use "ngfw" user on SCM to make REST API calls.

  There is no change to the existing SOFA protocol for file submission. Since a user called “ngfw” exists, all file submissions via the SOFA channel is assumed to be from McAfee NGFW appliances.

  Advanced Threat Defense is not able to support McAfee Network Security Platform and McAfee Next Generation Firewall in the same environment.

How the deployment options address the 4 major aspects of anti-malware process cycle:

- Detection of file download: As soon as a user accesses a file, the inline Network Security Platform Sensor or McAfee® Web Gateway detects this and sends a copy of the file to McAfee Advanced Threat Defense for analysis.
- Analysis of the file for malware: Even before the user fully downloads the file, McAfee Advanced Threat Defense can detect a known malware using sources that are local to it or on the cloud.
- Block future downloads of the same file: Every time McAfee Advanced Threat Defense detects a medium, high, or very high severity malware, it updates its local black list.
- Identify and remediate affected hosts: Integration with Network Security Platform enables you to quarantine the host until it is cleaned up and remediated.

Advanced Threat Defense advantages

Here are some of the advantages that Advanced Threat Defense provides:

- It is an on-premises solution that has access to cloud-based GTI. In addition, you can integrate it with other McAfee's security products.
- Advanced Threat Defense does not sniff or tap into your network traffic. It analyzes the files submitted to it for malware. This means that you can place the Advanced Threat Defense Appliance anywhere in your network as long as it is reachable to all the integrated McAfee products. It is also possible for one Advanced Threat Defense Appliance to cater to all such integrated products (assuming the number of files submitted is within the supported level). This design can make it a cost-effective and scalable anti-malware solution.
- Advanced Threat Defense is not an inline device. It can receive files from IPS Sensors for malware analysis. So, it is possible to deploy Advanced Threat Defense in such a way that you obtain the advantages of an inline anti-malware solution but without the associated drawbacks.
- Android is currently one of the top targets for malware developers. With this integration, the Android-based handheld devices on your network are also protected. You can dynamically analyze the files downloaded by your Android devices such as smartphones and tablets.
- Files are concurrently analyzed by various engines. So, it is possible for known malware to be blocked in almost real time.
- When Advanced Threat Defense dynamically analyzes a file, it selects the analyzer virtual machine that uses the same operating system and other applications as that of the target host. This is achieved through its integration with McAfee ePO or through passive device profiling feature of Network Security Platform. This enables you to identify the exact impact on a targeted host, so that you can take the required remedial measures. This also means that Advanced Threat Defense executes the file only the required virtual machine, reserving its resources for other files.
- Consider a host downloaded a zero-day malware, but a Sensor that detected this file downloaded submitted it to Advanced Threat Defense. After a dynamic analysis, Advanced Threat Defense determines the file to be malicious. Based on how you have configured the Advanced Malware policy, it is possible for the Manager to add this malware to the blacklist of all the Sensors in your organization's network. This file also might be on the blacklist of Advanced Threat Defense. Thus, the chances of the same file re-entering your network is reduced.
- Even the first time when a zero-day malware is downloaded, you can contain it by quarantining the affected hosts until they are cleaned and remediated.
- Packing can change the composition of the code or enable a malware to evade reverse engineering. So, proper unpacking is very critical to get the actual malware code for analysis. Advanced Threat Defense is capable of unpacking the code such that the original code is secured for static analysis.

2 Setting up the Advanced Threat Defense Appliance

Review this chapter for information regarding the Advanced Threat Defense Appliance and how to set it up.

Contents

About Advanced Threat Defense Appliance

Depending on the model, the Advanced Threat Defense Appliance is a 1-U or 2-U rack dense chassis with Intel® Xeon® E5-2600 product family processor. The McAfee Advanced Threat Defense Appliance runs on a pre-installed, hardened Linux kernel 3.6.0 and comes preloaded with the Advanced Threat Defense software.

The Advanced Threat Defense Appliance is available in the following models:

- ATD-3000: This standard model is a 1U chassis.
- ATD-6000: This high-end model is a 2U chassis.

Functions of a Advanced Threat Defense Appliance

The Advanced Threat Defense Appliances are purpose-built, scalable, and flexible high-performance servers designed to analyze suspicious files for malware.

The following are the primary functions of the Advanced Threat Defense Appliance:

- Host the Advanced Threat Defense software that analyzes files for malware.
- Host the Advanced Threat Defense web application.
- Host the virtual machines used for dynamic analysis of suspicious files.

For the performance values related to ATD-3000 and ATD-6000, contact McAfee support.

Before you install the Advanced Threat Defense Appliance

This section describes the tasks that you must complete before you begin to install a Advanced Threat Defense.

- Read all the provided documentation before installation.
- Make sure that you have selected a suitable location for installing the Advanced Threat Defense Appliance.
- Check that you have all the necessary equipment and components outlined in this document.
- Familiarize yourself with the McAfee Advanced Threat Defense Appliance network access card ports and connectors as described in this document.
- Make sure you have the following information available when you configure the Advanced Threat Defense Appliance:
  - IPv4 address that you want to assign to the Appliance.
  - Network mask.
  - Default gateway address.

Warnings and cautions

Read and follow these safety warnings when you install the Advanced Threat Defense Appliance. Failure to observe these safety warnings could result in serious physical injury.

> ⚠ Advanced Threat Defense Appliance power on/off — the push-button on/off power switch on the front panel of the Advanced Threat Defense Appliance does not turn off the AC power. To remove AC power from the Advanced Threat Defense Appliance, you must unplug the AC power cord from either the power supply or wall outlet for both the power supplies.

> ⚠ The power supplies in your system might produce high voltages and energy hazards, which can cause bodily harm. Only trained service technicians are authorized to remove the covers and access any of the components inside the system.

> ⚠ Hazardous conditions — devices and cables: Hazardous electrical conditions might be present on power, telephone, and communication cables. Turn off the Advanced Threat Defense Appliance and disconnect telecommunications systems, networks, modems, and both the power cords attached to the Advanced Threat Defense Appliance before opening it. Otherwise, personal injury or equipment damage can result.

> ⚠ Avoid injury — lifting the Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.

> ⚠ This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

> ⚠ Do not remove the outer shell of the Advanced Threat Defense Appliance. Doing so invalidates your warranty.

> ⚠ Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place. Blank faceplates and cover panels prevent exposure to hazardous voltages and currents inside the chassis, contain electromagnetic interference (EMI) that might disrupt other equipment and direct the flow of cooling air through the chassis.

> ⚠ To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

Usage restrictions

The following restrictions apply to the use and operation of Advanced Threat Defense Appliance:

- You should not remove the outer shell of the Advanced Threat Defense Appliance. Doing so invalidates your warranty.
- The Advanced Threat Defense Appliance is not a general purpose server.
- McAfee prohibits the use of Advanced Threat Defense Appliance for anything other than operating the Advanced Threat Defense solution.
- McAfee prohibits the modification or installation of any hardware or software on the Advanced Threat Defense Appliance that is not part of the normal operation of Advanced Threat Defense.

Unpack the shipment

1. Open the crate.
2. Remove the first accessory box.

3. Verify you have received all parts as listed in Check your shipment on page 22.
4. Remove the Advanced Threat Defense Appliance.
5. Place the Advanced Threat Defense Appliance as close to the installation site as possible.
6. Position the box with the text upright.
7. Open the top flaps of the box.
8. Remove the accessory box within the Advanced Threat Defense Appliance box.
9. Remove the slide rail kit.
10. Pull out the packing material surrounding the Advanced Threat Defense Appliance.
11. Remove the Advanced Threat Defense Appliance from the anti-static bag.
12. Save the box and packing materials for later use in case you need to move or ship the Advanced Threat Defense Appliance.

Check your shipment

The following accessories are shipped in the Advanced Threat Defense Appliance crate:

- Advanced Threat Defense Appliance
- Accessories itemized on the *Content Sheet*
- Set of tool-less slide rails
- Front bezel with key

McAfee Advanced Threat Defense Appliance front and back panels

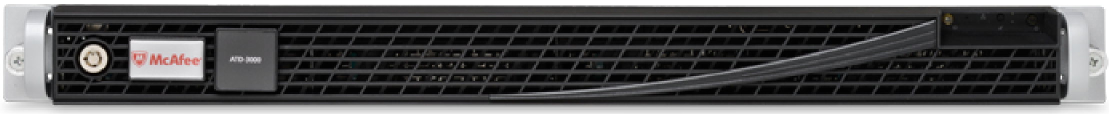


Figure 2-1 Front view of ATD-3000 with bezel

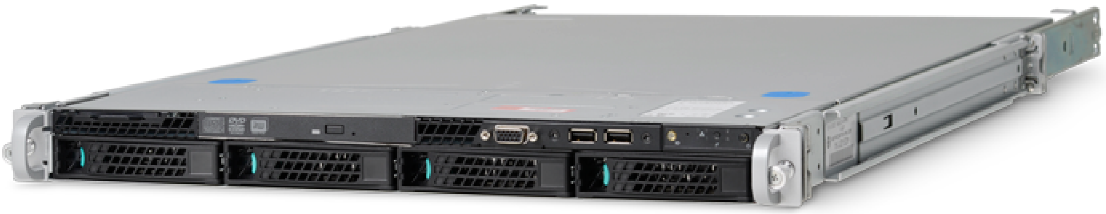


Figure 2-2 Side view of ATD-3000 without bezel

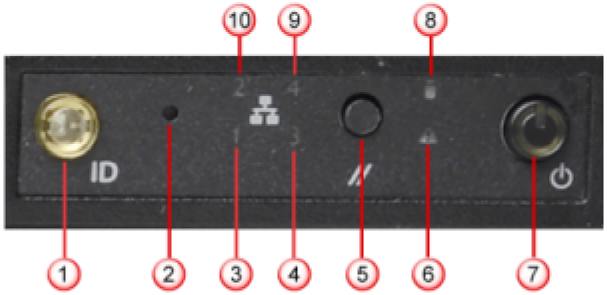


Figure 2-3 ATD-3000 and ATD-6000 front panel

Label	Description
1	System ID button with integrated indicator light
2	NMI button (recessed, tool required for use)
3	NIC 1 activity indicator light
4	• ATD-3000: NIC 3 activity indicator light • ATD-6000: Not used
5	System cold reset button
6	System status indicator light
7	Power button with integrated indicator light
8	Hard drive activity indicator light
9	• ATD-3000: NIC 4 activity indicator light • ATD-6000: Not used
10	NIC 2 activity indicator light

An optional, lockable bezel is included with the McAfee Advanced Threat Defense Appliance, which you can install to cover the front panel.

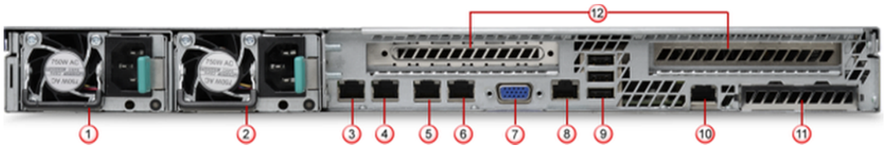


Figure 2-4 ATD-3000 Appliance back panel

Label	Description
1	Power supply module 1
2	Power supply module 2
3	Management port (NIC 1). This is the eth-0 interface. The `set appliance` and `set mgmtport` commands apply to this interface. For example, when you use the `set appliance ip` command, the corresponding IP address is assigned to this interface.
4	NIC 2. This is the eth-1 interface. This interface is disabled by default. • To enable or disable this interface, use the `set intfport` command. For example, `set intfport 1 enable` • To assign the IP details to this interface use `set intfport <eth 1, 2, or 3> ip <IPv4 address> <subnet mask>` For example, `set intfport 1 ip 10.10.10.10 255.255.255.0` • You cannot assign the default gateway to this port. However, you can configure a route on this interface to route the traffic to the desired gateway. To configure a route, use `route add network <IPv4 subnet> netmask <netmask> gateway <IPv4 address> intfport 1` For example, `route add network 10.10.10.0 netmask 255.255.255.0 gateway 10.10.10.1 intfport 1`. This command routes all traffic from the 10.10.10.0 command to 10.10.10.1 through NIC 2 (eth-1).
5	NIC 3. This is the eth-2 interface. The note described for NIC 2 applies to this interface as well.
6	NIC 4. This is the eth-3 interface. The note described for NIC 2 applies to this interface as well.
7	Video connector

Label	Description
8	RJ45 serial-A port
9	USB ports
10	RMM4 NIC port
11	I/O module ports/connectors (not used)
12	Add-in adapter slots from riser card 1 and riser card 2

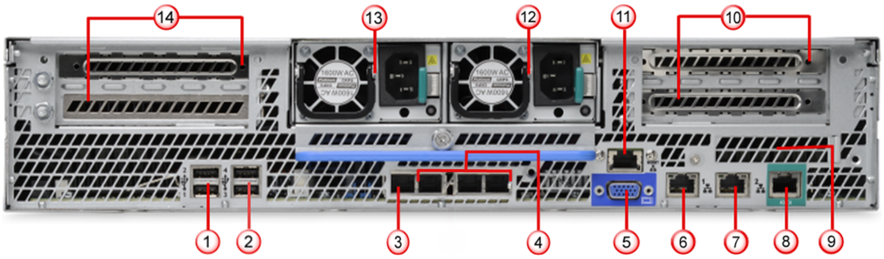


Figure 2-5 ATD-6000 Appliance back panel

Label	Description
1	USB ports
2	USB ports
3	Management port. This is the eth-0 interface. The `set appliance` and `set mgmtport` commands apply to this interface. For example, when you use the `set appliance ip` command, the corresponding IP address is assigned to this interface.
4	Additional I/O module ports/connectors. These are the eth-1, eth-2, and eth-3 interfaces respectively. These interfaces are disabled by default. • To enable or disable an interface, use the `set intfport` command. For example, `set intfport 1 enable` to enable eth-1. • To assign the IP details to an interface use `set intfport <eth 1, 2, or 3> ip <IPv4 address> <subnet mask>` For example, `set intfport 1 ip 10.10.10.10 255.255.255.0` • You cannot assign the default gateway to this port. However, you can configure a route on this interface to route the traffic to the desired gateway. To configure a route, use `route add network <IPv4 subnet> netmask <netmask> gateway <IPv4 address> intfport 1` For example, `route add network 10.10.10.0 netmask 255.255.255.0 gateway 10.10.10.1 intfport 1`. This command routes all traffic from the 10.10.10.0 command to 10.10.10.1 through eth-1.
5	Video connector
6	NIC 1 (currently not used)
7	NIC 2 (currently not used)
8	RJ45 serial-A port
9	I/O module ports/connectors (not used)
10	Add-in adapter slots from riser card
11	RMM4 NIC port
12	Power supply module 2
13	Power supply module 1
14	Add-in adapter slots from riser card

Hardware specifications and environmental requests

Specifics	ATD-3000	ATD-6000
Dimensions	• 734.66 L x 438 W x 43.2 H in millimeters • 29 L x 17.25 W x 1.70 H in inches	• 712 L x 438 W x 87.3 H in millimeters • 28 L x 17.24 W x 3.43 H in inches
Form Factor	1U rack mountable; fits 19-inch rack	2U rack mountable; fits 19-inch rack
Weight	15 Kg (33 lbs)	22.7 Kg (50 lbs.)
Storage	• Disk space HDD: 2 x 4TB • SSD: 2 x 400 GB	• Disk space HDD: 4 x 4TB • SSD: 2 x 800 GB
Maximum Power Consumption	2x 750W	2x 1600W
Redundant Power Supply	AC redundant, hot swappable	AC redundant, hot swappable
AC voltage	100 - 240 V at 50 - 60 Hz. 5.8 Amps	100 - 240 V. 50 - 60 Hz. 8.5 Amps
Operating Temperature	+10°C to +35° C (+50°F to + 95°F) with the maximum rate of change not to exceed 10°C per hour	+10º C to +35º C (+50ºF to +95ºF) with the maximum rate of change not to exceed 10°C per hour
Non-operating temperature	-40°C to +70°C (-40°F to +158°F)	-40°C to +70°C (-40°F to +158°F)
Relative humidity (non-condensing)	• Operational: 10% to 90% • Non-operational: 90% at 35°C	• Operational: 10% to 90% • Non-operational: 50% to 90% with a maximum wet bulb of 28°C (at temperatures from 25°C to 35°C)
Altitude	Support operation up to 3050 meters (10,000 feet)	Support operation up to 3050 meters (10,000 feet)
Safety Certification	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations	UL 1950, CSA-C22.2 No. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB license and report covering all national country deviations
EMI Certification	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)	FCC Part 15, Class A (CFR 47) (USA) ICES-003 Class A (Canada), EN55022 Class A (Europe), CISPR22 Class A (Int'l)
Acoustic noise	Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees C).	Sound power: 7.0 BA in operating conditions at typical office ambient temperature (23 +/- 2 degrees °C).
Shock, operating	Half sine, 2 g peak, 11 milliseconds	Half sine, 2 g peak, 11 milliseconds
Shock, unpackaged	Trapezoidal, 25 g, velocity change 136 inches/second (≧40 lbs to < 80 lbs)	Trapezoidal, 25 g, velocity change is based on packaged weight

Specifics	ATD-3000	ATD-6000
Shock, packaged	Non-palletized free fall in height 24 inches (≧40 lbs to < 80 lbs)	• Product Weight: ≥ 40 to < 80 • Non-palletized Free Fall Height = 18 inches • Palletized (single product) Free Fall Height = NA
Vibration	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random Packaged: 5 Hz to 500 Hz, 1.09 g RMS random
ESD	+/-12 KV except I/O port +/- 8 KV per Intel® Environmental test specification	Air Discharged: 12.0 kV Contact Discharge: 8.0 kV
System cooling requirement in BTU/Hr	• 460 Watt Max – 1570 BTU/hour • 750 Watt Max – 2560 BTU/hour	• 460 Watt Max – 1570 BTU/hour • 750 Watt Max – 2560 BTU/hour
Memory	192 GB	256 GB

Port numbers

Table 2-1 Port numbers

Client	Server	Default port	Configurable	Description
Any (desktop)	Advanced Threat Defense	TCP 443 (HTTPS)	No	Access Advanced Threat Defense web application
Any (FTP client)	Advanced Threat Defense	TCP 22 (SFTP)	No	Access the FTP server on Advanced Threat Defense
Sensor	Advanced Threat Defense	TCP 8505	No	Communication channel between a Sensor and Advanced Threat Defense
Manager	Advanced Threat Defense	TCP 443 (HTTPS)	No	Communication between the Manager and Advanced Threat Defense through the RESTful APIs.
Advanced Threat Defense	McAfee ePO	TCP 8443	Yes	Host information queries.
Advanced Threat Defense	`tunnel.message.trustedsource.org`	TCP 443 (HTTPS)	No	File Reputation queries.
Advanced Threat Defense	`List.smartfilter.com`	TCP 80 (HTTP)	No	URL updates.
Any (SSH client)	Advanced Threat Defense	TCP 2222 (SSH)	No	CLI access
Advanced Threat Defense	`wpm.webwasher.com`	TCP 443 (HTTPS)	No	Updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine.

Setting up Advanced Threat Defense

This chapter describes how to set up the Advanced Threat Defense Appliance for you to configure it.

Contents

Install or remove rack handles

- To install a rack handle, align it with the two holes on the side of the Advanced Threat Defense Appliance and attach the rack handle to the Appliance with two screws as shown.

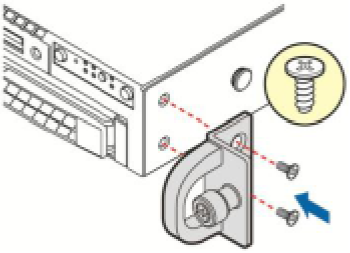


Figure 2-6 Installing the rack handle

- To remove a rack handle, remove the two screws holding the rack handle in place, and remove the rack handle from the server system as shown.

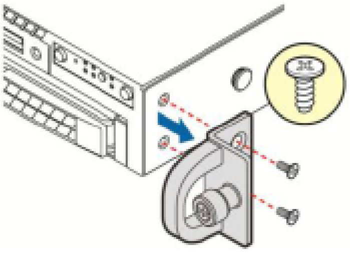


Figure 2-7 Removing the rack handle

Install or remove the Appliance from the rack

Use the rack-mounting kit included with the Advanced Threat Defense Appliance to install the unit into a four-post 19-inch rack. The kit can be used with most industry-standard rack cabinets. Use the tie wraps to secure the cables from the Advanced Threat Defense Appliance to the rack.

Task

1. At the front of the rack, position the right or the left mounting rail on the corresponding side so that its mounting bracket aligns with the required rack holes.

   > Ensure that you follow the safety warnings. When identifying where you want the Advanced Threat Defense Appliance to go in the rack, remember that you should always load the rack from the bottom up. If you are installing multiple Advanced Threat Defense Appliance, start with the lowest available position first.

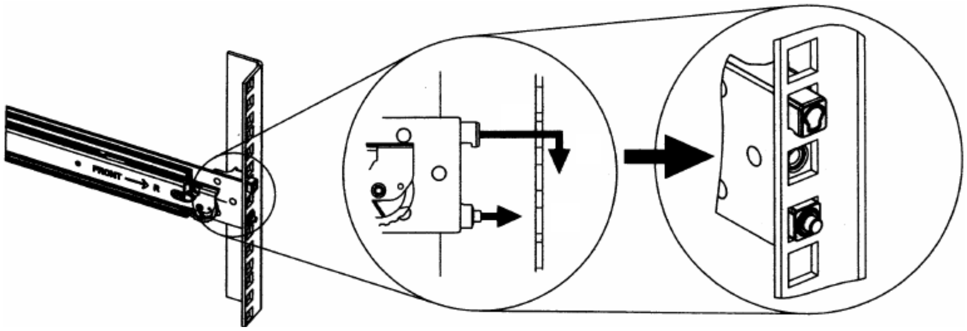


Figure 2-8 Slide rail installation

2. At the back of the rack, pull the back mounting-bracket (extending the mounting rail) so that it aligns with the required rack holes.

   > Ensure that the mounting rails are at the same level on each side of the rack.

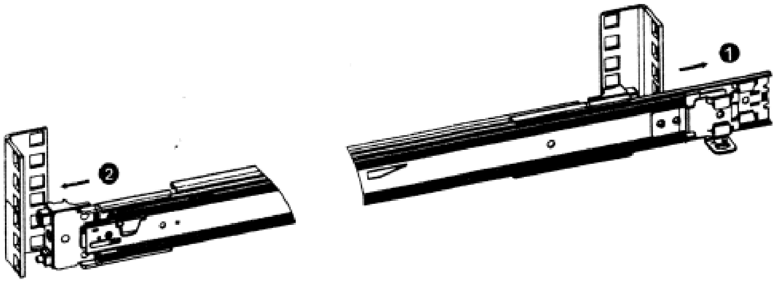


Figure 2-9 Install rail to rack

3. Clip the rail to the rack and secure it.

4. Repeat these steps to secure the second mounting rail to the rack.

5 Slide both the rails to full extent.

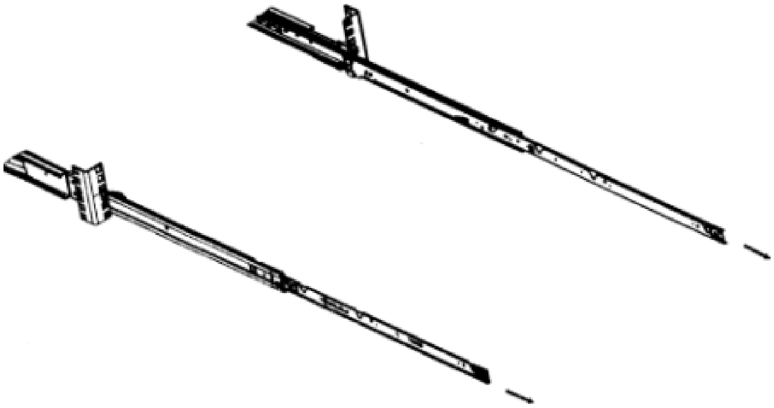


Figure 2-10 Full extend slide

6 With help from another person, lift the Advanced Threat Defense Appliance and install the chassis to the rail simultaneously on both the sides.

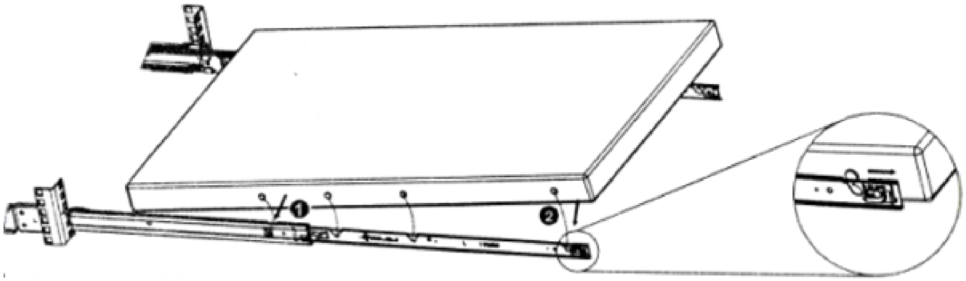


Figure 2-11 Install the Appliance to rail

Drop in the rear spool first, followed by the middle and then front.

> Lifting the Advanced Threat Defense Appliance and attaching it to the rack is a two-person job.

7 Attach the lockable bezel to protect the front panel if required.

8 Lift the release tab and push the Appliance into the rack.

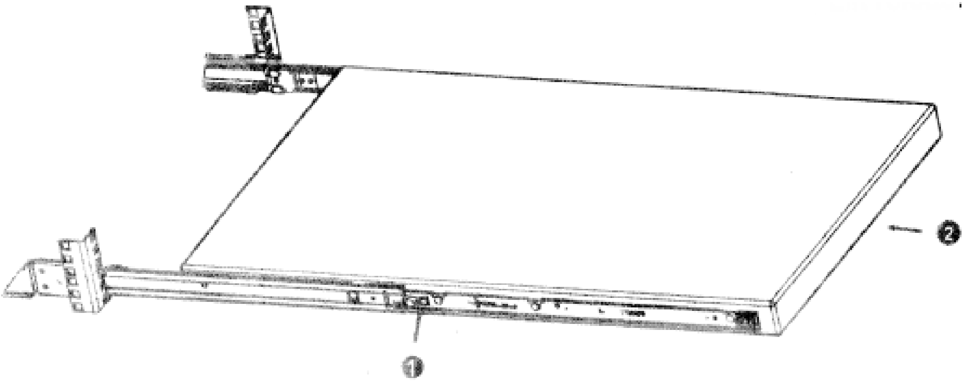


Figure 2-12 Lift release tab and push Appliance into rack

9 To remove the Advanced Threat Defense Appliance from the rack, lift the release tab next to the front spool on the chassis and lift it out of the rails.

This needs to be done simultaneously on both the sides and requires two people.

Turn on the McAfee Advanced Threat Defense Appliance

The Advanced Threat Defense Appliance has redundant power supplies pre-installed.

> The Advanced Threat Defense Appliance ships with two power cords specific to your country or region.

Task

1. Plug one end of the AC power cord into the first power supply module in the back panel and the other end into an appropriate power source.
2. Plug one end of the AC power cord into the second power supply module in the back panel and the other end into an appropriate power source. Advanced Threat Defense powers up without pressing the on/off button on the front panel.

   > The on/off button on the front panel does not turn on/off the AC power. To remove AC power from the Advanced Threat Defense Appliance, you must unplug both AC power cords from either the power supply or wall outlet.

Handling the front bezel

You can remove the front bezel if required, and then re-install it. However, before you install the bezel, you must install the rack handles.

Task

1. Follow these steps to remove the front bezel.
   a. Unlock the bezel if it is locked.
   b. Remove the left end of front bezel from rack handle.
   c. Rotate the front bezel anticlockwise to release the latches on the right end from the rack handle.

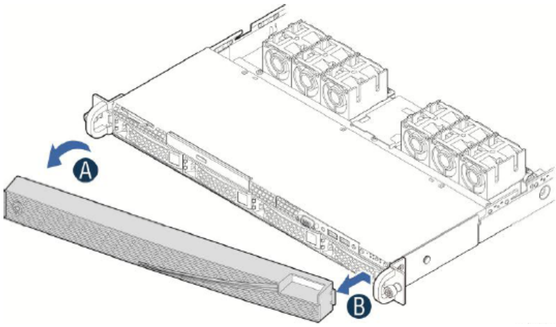


Figure 2-13 Removing front bezel

2. Follow these steps to install the front bezel.
   a. Lock the right end of the front bezel to the rack handle
   b. Rotate the front bezel clockwise until the left end clicks into place
   c. Lock the bezel if needed.

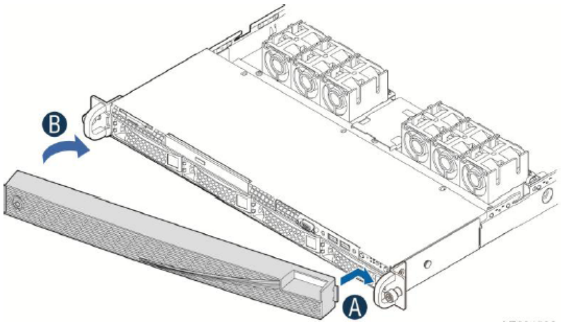


Figure 2-14 Installing front bezel

Connect the network cable

Task

1. Plug a Category 5e or 6 Ethernet cable in the management port, which is located in the back panel.
2. Plug the other end of the cable into the corresponding network device.

Configure network information for Advanced Threat Defense Appliance

After you complete the initial installation and configuration, you can manage the Advanced Threat Defense Appliance from a remote computer or terminal server. To do so, you must configure the Advanced Threat Defense Appliance with the required network information.

Task

1. Plug a console cable (RJ45 to DB9 serial) to the console port (RJ45 serial-A port) at the back panel of the Advanced Threat Defense Appliance.

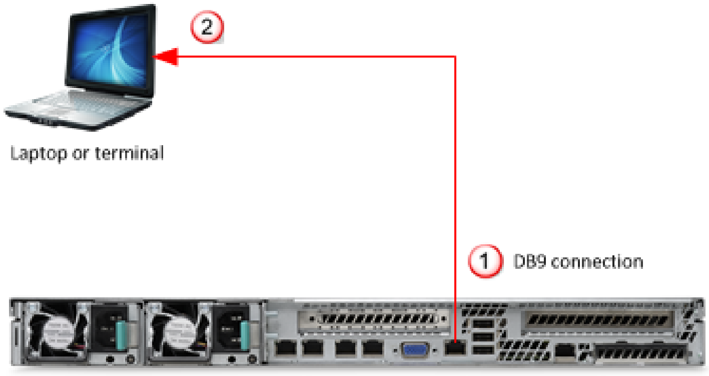


Figure 2-15 Connect the console port

2. Connect the other end of the cable directly to the COM port of the computer or port of the terminal server you are using to configure the Advanced Threat Defense Appliance.

3 Run the HyperTerminal from a Microsoft Windows-based computer with the following settings.

Name	Setting
Baud rate	115200
Number of Bits	8
Parity	None
Stop Bits	1
Control Flow	None

4 At the logon prompt, log on to the Advanced Threat Defense Appliance using the default user name `cliadmin` and password `atdadmin`.

> You can type `help` or `?` to access instructions on using the built-in command syntax help. For a list of all commands, type `list`.

5 At the command prompt, type `set appliance name <Name>` to set the name of the Advanced Threat Defense Appliance.

> You need to type the values between <> characters, excluding the <> characters.

Example: `set appliance name matd_appliance_1`

The Advanced Threat Defense Appliance name can be an alphanumeric character string up to 25 characters. The string must begin with a letter and can include hyphens, underscores, and periods, but not spaces.

6 To set the management port IP address and subnet mask of the Advanced Threat Defense Appliance, type `set appliance ip <A.B.C.D> <E.F.G.H>`

Specify a 32-bit address written as four eight-bit numbers separated by periods as in <A.B.C.D>, where A, B, C, or D is an eight-bit number between 0-255. <E.F.G.H> represents the subnet mask.

Example: `set appliance ip 10.34.2.8 255.255.255.0`

> Advanced Threat Defense Appliance must not be assigned the following three class C network IP addresses:
>
> - `192.168.50.0/24`
> - `192.168.55.0/24`
> - `192.168.88.0/24`

> After you set the IP address the first time or when you modify the IP address, you must restart the Advanced Threat Defense Appliance.

7 Set the address of the default gateway.

```
set appliance gateway <A.B.C.D>
```

Use the same convention as for the `set appliance ip` command.

Example: `set appliance gateway 12.34.2.1`

8 Set the port speed and duplex settings for the management port using one of the following commands:

- `set mgmtport auto` — Sets the management port in auto mode for speed and duplex.
- `set mgmtport speed (10|100) duplex (full|half)` — Sets the speed to 10 or 100 Mbps at full or half duplex.

9 To verify the configuration, type `show`.

This displays the current configuration details.

10 To check the network connectivity, ping other network hosts. At the prompt, type `ping <IP address>`

The success message `host <ip address> is alive` appears. If the host is not reachable, `failed to talk to <ip address>` appears.

11 Change the Advanced Threat Defense Appliance password by using the `passwd` command.

A password must be between 8 and 25 characters, is case sensitive, and can consist of any alphanumeric character or symbol.

> McAfee strongly recommends that you choose a password with a combination of characters that is easy for you to remember but difficult for someone else to guess.

12 Reboot the ATD appliance.

> At any point of time, if you change the IP address of ATD, you must reboot the appliance to reflect the changes.

3 Accessing Advanced Threat Defense web application

The Advanced Threat Defense web application is hosted on the Advanced Threat Defense Appliance. If you are a Advanced Threat Defense user with web access, you can access the Advanced Threat Defense web application from a remote machine using a supported browser.

Using the Advanced Threat Defense web application, you can:

- Monitor the state and performance of the Advanced Threat Defense Appliance.
- Manage Advanced Threat Defense users and their permissions.
- Configure Advanced Threat Defense for malware analysis.
- Manually upload files to be analyzed.
- Monitor the progress of the analysis and subsequently view the results.

Contents

McAfee Advanced Threat Defense client requirements

The following are the system requirements for client systems connecting to the Advanced Threat Defense web application.

- Client operating system — Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows 7, and Microsoft Windows 8.0
- Browsers — Internet Explorer 10 and later, Google Chrome 40.0.2214.115 to 46.0.2490.71, and Mozilla Firefox 36.0.4 to 41.0.2.

Browser settings for HTML5 support

User-interactive mode (XMode) is used for activation of VM images and manual submission of files. This mode works with any browser that support HTML5 Canvas. You do not need to install Java to use the XMode feature.

Google Chrome version 44.0.2403 and higher and Mozilla Firefox version 40.0.3 and higher are supported. Microsoft Internet Explorer is not supported.

You need to modify Firefox settings to use the HTML5 feature.

1. From the Firefox Home page, click **Options** | **Advanced** | **Certificates** | **View Certificates**.
2. From the Certificate Manager window, click **Servers**.
3. Click **Add Exception...** and type `https://<Host ATD IP address>:6080` and click **Get Certificate**.
4. Click **Confirm Security Exception** and then **OK**.
5. Click **Activation** or **XMode**.

Access the Advanced Threat Defense Appliance web application

Task

1. From a client computer, open a session using one of the supported browsers.
2. Use the following to access the Advanced Threat Defense web application:
   - URL — https://<Advanced Threat Defense Appliance host name or IP address>
   - Default user name — `admin`
   - Password — `admin`
3. Click **Log In.**
4. A new window appears prompting admin user to change the administrator default password. Change the default password.

4 Managing Advanced Threat Defense

You use the Advanced Threat Defense web application to manage configurations such as user accounts and to monitor the Advanced Threat Defense Appliance's system health.

Contents

Managing McAfee Advanced Threat Defense users

You can create user accounts for McAfee Advanced Threat Defense with different permissions and configuration settings. These permissions and settings depend on the user's role with respect to malware analysis using McAfee Advanced Threat Defense. Using the McAfee Advanced Threat Defense web application, you can create user accounts for:

- Users who use the McAfee Advanced Threat Defense web application for submitting files for analysis and for viewing the results of the analysis.
- Users who upload the files to the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
- Users who directly use the RESTful APIs for uploading files. For more information, see the *McAfee Advanced Threat Defense RESTful APIs Reference Guide.*

In the user record, you also specify the default analyzer profile. If you are using the McAfee Advanced Threat Defense web application to upload, you can override this selection when you actually upload a file.

For each user, you can also configure the FTP server details to which you want McAfee Advanced Threat Defense to upload the results of the analysis.

- There are five default user records.
  - Default Admin — This is the default super-user account. You can use this account to initially configure the McAfee Advanced Threat Defense web application. The logon name is *admin* and the default password is *admin*. User is forced to change the default password after logon.
  - Network Security Platform — The logon name is *nsp* and the default password is *admin*. This is used by Network Security Platform to integrate with McAfee Advanced Threat Defense.
  - ATD upload Admin — This is the default user account to access the FTP server on McAfee Advanced Threat Defense. The user name is *atdadmin* and the password is *atdadmin.*

    - McAfee Web Gateway — This is for the integration between McAfee Web Gateway and McAfee Advanced Threat Defense.
    - McAfee Email Gateway — This is for the integration between McAfee Email Gateway and McAfee Advanced Threat Defense.

- To access the CLI of McAfee Advanced Threat Defense, you must use *cliadmin* as the logon name and *atdadmin* as the default password. User is forced to change the default password after logon. You cannot access this user record. You cannot create any other user to access the CLI.

  > You access the CLI through SSH over port 2222. See Log on to the CLI on page 345.

- If you are not an admin user, you can view your user record and modify it. To modify your role assignments, you must contact the admin user.

> Multiple login for admin users is allowed only when McAfee Advanced Threat Defense is in non-CC mode. The same is not allowed in CC mode.

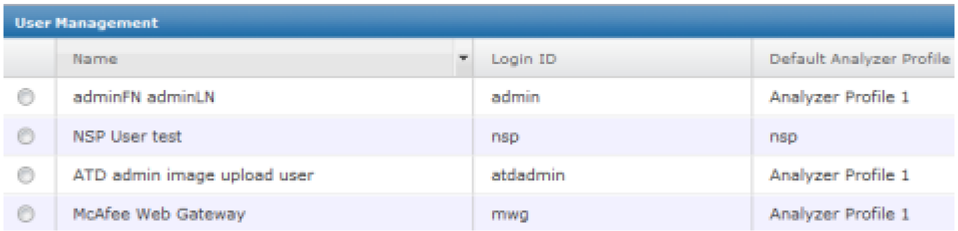
Viewing user profiles

If you are a user with admin role, you can view the existing list of McAfee Advanced Threat Defense users. If you do not have admin role, you can view your user record.

Task

1 Select **Manage** | **User Management**.

The current list of users is displayed (based on your role).



User Management

	Name	Login ID	Default Analyzer Profile
○	adminFN adminLN	admin	Analyzer Profile 1
○	NSP User test	nsp	nsp
○	ATD admin image upload user	atdadmin	Analyzer Profile 1
○	McAfee Web Gateway	mwg	Analyzer Profile 1

Figure 4-1 View the list of users

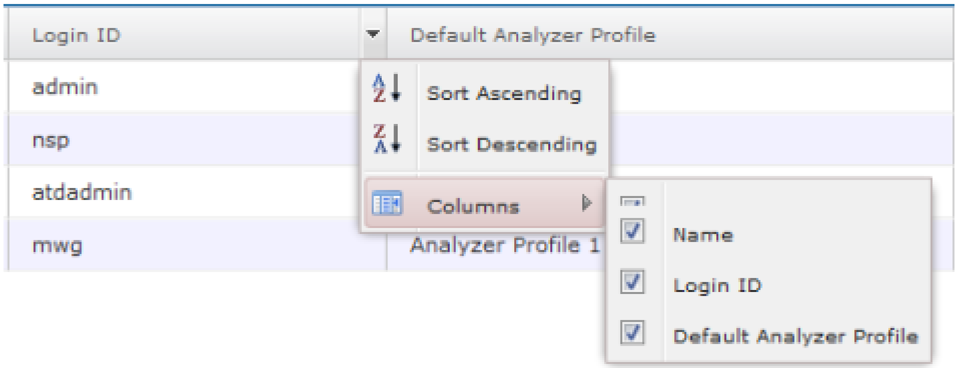
Column name	Definition
Select	Select to edit or delete the user record.
Name	Full name of the user as entered in the user details.
Login ID	The user name for accessing McAfee Advanced Threat Defense.
Default Analyzer Profile	The Analyzer Profile that McAfee Advanced Threat Defense uses when the user submits a sample for analysis. However, the user can override this at the time of sample submission.

2 Hide the columns you do not want to see.

   a Move the mouse over the right corner of a column heading and click the drop-down arrow.

   b Select **Columns**.

   c Select only the required column names from the list.



Login ID	Default Analyzer Profile
admin	
nsp	
atdadmin	
mwg	Analyzer Profile 1

Figure 4-2 Select the required column names

3 To sort the user records list based on a particular column name, click the column heading.

   You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific user, select the record and click **Edit**.

Add users

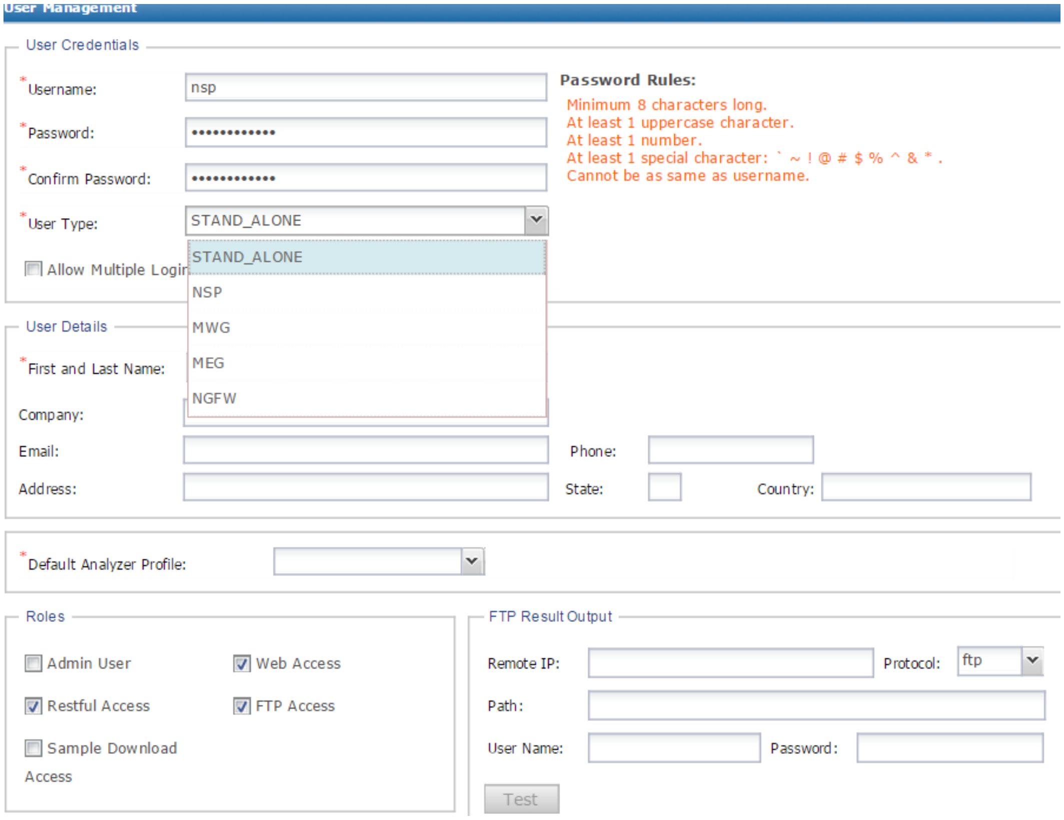
If you have the *admin user* role, you can create the following types of users:

- Users with admin role in the McAfee Advanced Threat Defense web application
- Non-admin users in the McAfee Advanced Threat Defense web application
- Users with access to the FTP server hosted on the McAfee Advanced Threat Defense Appliance.
- Access to the RESTful APIs of the McAfee Advanced Threat Defense web application

Task

1 Select **Manage** | **User Management** | **New.**

The **User Management** page is displayed.



User Management

User Credentials

*Username: nsp

*Password: ••••••••••••

*Confirm Password: ••••••••••••

*User Type: STAND_ALONE

STAND_ALONE
NSP
MWG
MEG
NGFW

□ Allow Multiple Login

Password Rules:

Minimum 8 characters long.
At least 1 uppercase character.
At least 1 number.
At least 1 special character: ` ~ ! @ # $ % ^ & * .
Cannot be as same as username.

User Details

*First and Last Name:

Company:

Email:

Phone:

Address:

State:

Country:

*Default Analyzer Profile:

Roles

□ Admin User

☑ Web Access

☑ Restful Access

☑ FTP Access

□ Sample Download Access

FTP Result Output

Remote IP:

Protocol: ftp

Path:

User Name:

Password:

Figure 4-3 Add users

2 Enter the appropriate information in the respective fields.

Option name	**Definition**
Username	The user name for accessing the McAfee Advanced Threat Defense web application, FTP server, or RESTful APIs.
Password	The default password that you want to provide to the user. It must meet the following criteria: • Minimum 8 characters in length. • At least one of the alphabetic characters must be in uppercase. • Must contain at least 1 number. • Must contain at least one of the following special characters ` ~ ! @ # $ % ^ & * • Password and user name must not be same.
Allow Multiple Logins	Deselect it you want to restrict the concurrent logon sessions for this user name to just one. Select if you want to allow multiple concurrent logon sessions for the user name.
First and Last Name	Enter the full name of the user. It must be of at least 2 characters in length.
Email	Optionally, enter the email address of the user.

Option name	Definition
Company	Optionally, enter the organization to which the user belongs.
Phone	Optionally, enter the user's phone number.
Address	Optionally, enter the user's address for communication.
State	Optionally, enter the corresponding State for the address you entered.
Country	Optionally, enter the corresponding Country for the address you entered.
Default Analyzer Profile	Select the analyzer profile that must be used for files submitted by the user. Users, who manually submit files, can override this setting by selecting a different analyzer profile at the time of file submission.
User Type	Select user type from the drop-down list. For example, select NSP if you want to submit samples using Network Security Platform Sensor.
Roles	• **Admin User —** Select to assign super-user rights in the McAfee Advanced Threat Defense web application. Users with this role can access all menus and create other users. • **Web Access —** This role enables a user to submit files using the McAfee Advanced Threat Defense web application and view the results. Users with this role can access all features but can only view their own user profile. Also, when they manually submit files, they can assign only the analyzer profiles that they created. • **FTP Access —** Select to assign access to the FTP server hosted on the McAfee Advanced Threat Defense Appliance to submit files for analysis. You must login to the FTP server as **atdadmin** user before uploading VMDK file to the McAfee Advanced Threat Defense Appliance. • **Log User Activities —** Select if you want to log the changes made by the user in the McAfee Advanced Threat Defense web application. • **Restful Access —** Select to assign access to the RESTful APIs of the McAfee Advanced Threat Defense web application to submit files for analysis. The **Restful Access** role must be selected for the integrated McAfee products that use RESTful APIs. If you remove this selection, the integration might not work. • **Sample Download Access —** This role enables a user to download originally submitted samples.

Option name	Definition
FTP Result Output	Specify the details of the FTP server to which McAfee Advanced Threat Defense must provide the results of malware analysis. When you configure the FTP server details, McAfee Advanced Threat Defense sends the results to the specified FTP server as well as stores in its data disk. When the data disk is 75 percent full, the older analysis results are deleted. To preserve the results for a longer term, you can configure **FTP Result Output**. • **Remote IP** — The IPv4 address of the FTP server. • **Protocol** — Specify whether FTP or SFTP must be used. McAfee recommends using SFTP. • **Path** — The complete path to the folder where the results must be saved. • **User Name** — The user name that McAfee Advanced Threat Defense must use to access the FTP server. • **Password** — The password for accessing the FTP server. • **Test** — to verify if McAfee Advanced Threat Defense is able to communicate with the specified FTP server using the specified protocol (FTP or SFTP).
Save	Creates the user record with the information you provided. If you configure an FTP server for result output, make sure that the test connection is successful before you click **Save**.
Cancel	Closes the **User Management** page without saving the changes.

Edit Users

If you are assigned the admin-user role, you can edit the user profiles. If you intend to modify the mandatory fields, then as a best practice, make sure the corresponding user is not logged on. If you are assigned only the web-access or Restful-access roles, only your user profile is available for editing.

Task

1 Select **Manage** | **User Management**.

The current list of users is displayed.

2 Select the required user record and click **Edit**.

The **User Management** page is displayed.

3 Make the changes to the required fields and click **Save**.

For information on the fields, see Add users on page 39.

Delete Users

If you are assigned the admin-user role, you can delete user records. Make sure that the corresponding user is not logged on.

> You cannot delete any predefined user records, which are the admin user record, the user record for Network Security Platform, and the user record for McAfee Web Gateway.

Task

1 Select **Manage** | **User Management**.

The current list of users is displayed.

2. Select the required user record and click **Delete**.
3. Click **Yes** to confirm deletion.

Monitoring the Advanced Threat Defense performance

You can use the following options to monitor the performance of Advanced Threat Defense.

- Use the monitors on the Advanced Threat Defense dashboard to continuously monitor the performance. See Advanced Threat Defense performance monitors on page 317.
- Use the `status` command in the Advanced Threat Defense Appliance CLI. See CLI commands for McAfee Advanced Threat Defense on page 6.

Upgrade Advanced Threat Defense and Android VM

This section provides information on how to upgrade the Advanced Threat Defense version as well as the Android version for the default Android analyzer VM.

> We strongly recommend you to upgrade your Advanced Threat Defense software to 3.4.2.32 or a later version.

Following are the upgrade paths to upgrade Advanced Threat Defense software to 3.4.8.

- If the current version is below than 3.4.2.32 and you want to upgrade to 3.4.8, you upgrade the Advanced Threat Defense to 3.4.2.32 or above and then upgrade to 3.4.8.
- If the current version is 3.4.2.32, you can directly upgrade to 3.4.8. See Upgrade ATD software from 3.4.2.32 to 3.4.8 on page 44.
- If the current version is 3.4.4.63, you can directly upgrade to 3.4.8. See Upgrade ATD software from 3.4.4.63 to 3.4.8 on page 46.
- If the current version is 3.4.6, you can directly upgrade to 3.4.8. See Upgrade ATD software from 3.4.6 to 3.4.8 on page 48.

> Once you upgrade, you cannot downgrade by loading the backup image using the `reboot backup` command.

> Once you upgrade to 3.4.8, you cannot downgrade by using *system.msu* files.

> Once you upgrade to 3.4.8, OpenSSL 1.0.1J is upgraded to OpenSSL 1.0.1m

> Once you upgrade to 3.4.8, use `copyto backup` command to ensure that the Active disk and Backup disk remain on the same software version of Advanced Threat Defense.

> Boot from Backup disk is not supported in case the Backup disk and Active disk reside at different software versions of Advanced Threat Defense.

The Android version in the default Android analyzer VM is 4.3.

Upgrade ATD software from 3.4.2.32 to 3.4.8

Before you begin

- Make sure that the current version of Advanced Threat Defense is 3.4.2.32.
- Make sure that the *system-3.4.8.msu* Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the Advanced Threat Defense web application.
- You have the credentials to log on to the Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Task

1. Log on to the Advanced Threat Defense Appliance using an FTP client such as FileZilla.

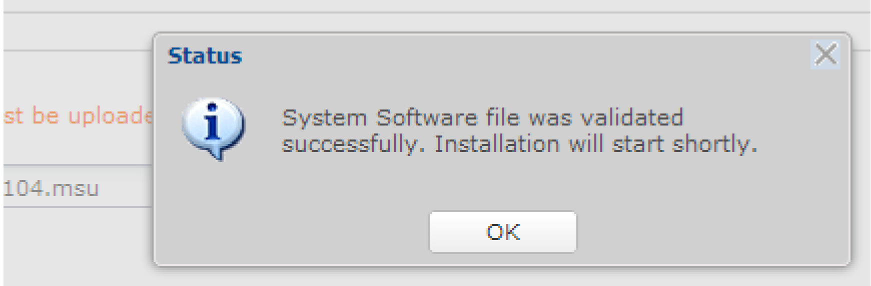
   Log on as the atdadmin user.

2. Using SFTP, upload the system-<version number>.msu file to the root directory of Advanced Threat Defense.

   Make sure that the transfer mode is binary.

3. After the file is uploaded, log on to the Advanced Threat Defense web application as the admin user and select **Manage | Software Management**.
4. Under **System Software**, select the system-<version number>.msu file.
5. Make sure that **Reset Database** is deselected in case of upgrades and click **Install**.

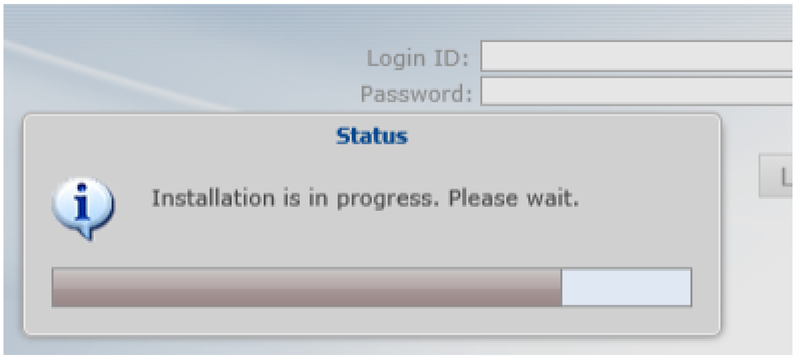
6 A confirmation message is displayed; click **OK**.



Status

System Software file was validated successfully. Installation will start shortly.

The system software is installed and the status is displayed in the browser.



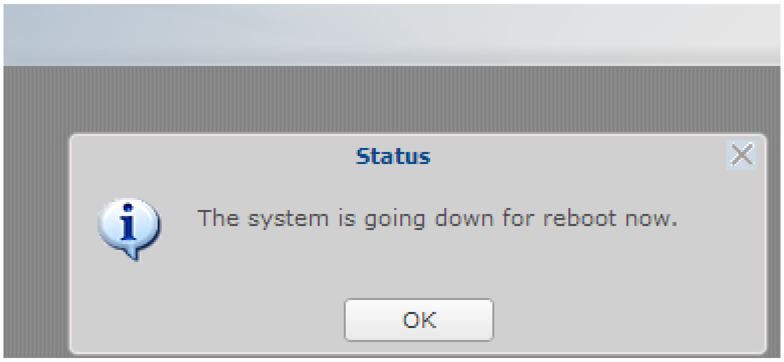
Status

Installation is in progress. Please wait.

It takes a minimum of 20 minutes for the system software installation to complete.

7 After the software is installed Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.



Status

The system is going down for reboot now.

If you are not able to view these messages, clear the browser cache.

8 Wait for Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

9 Verify the version in the Advanced Threat Defense web application.

10 Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

> When you upgrade to Advanced Threat Defense 3.4.8, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

11 Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of Advanced Threat Defense Appliance.

> Whitelist status is disabled after you upgrade to Advanced Threat Defense 3.4.8.

Upgrade ATD software from 3.4.4.63 to 3.4.8

Before you begin

- Make sure that the current version of Advanced Threat Defense is 3.4.4.63.
- Make sure that the *system-3.4.8.msu* Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the Advanced Threat Defense web application.
- You have the credentials to log on to the Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Task

1 Log on to the Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

2 Using SFTP, upload the system-<version number>.msu file to the root directory of Advanced Threat Defense.

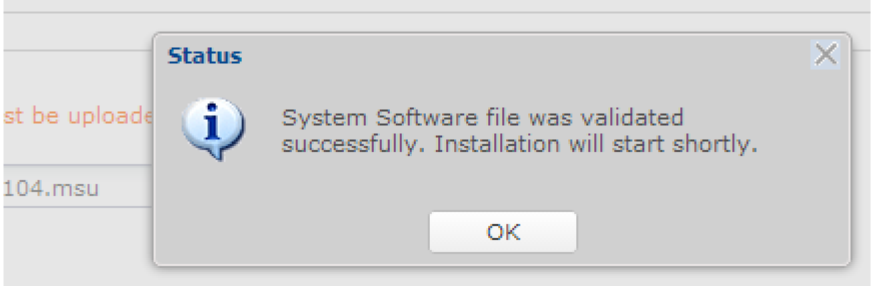
> Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

4 Under **System Software**, select the system-<version number>.msu file.

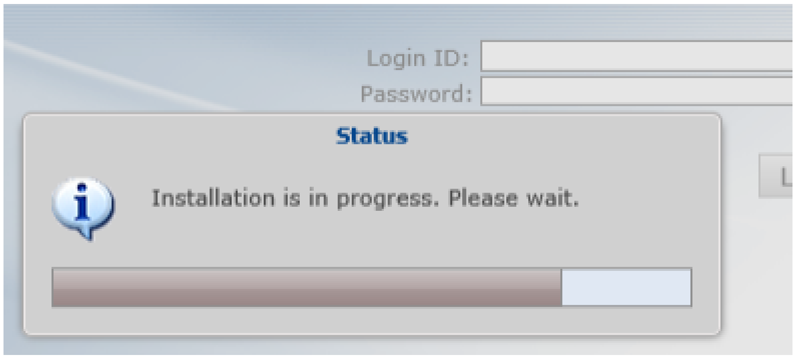
5 Make sure that **Reset Database** is deselected in case of upgrades and click **Install**.

6 A confirmation message is displayed; click **OK**.



System Software file was validated successfully. Installation will start shortly.

The system software is installed and the status is displayed in the browser.

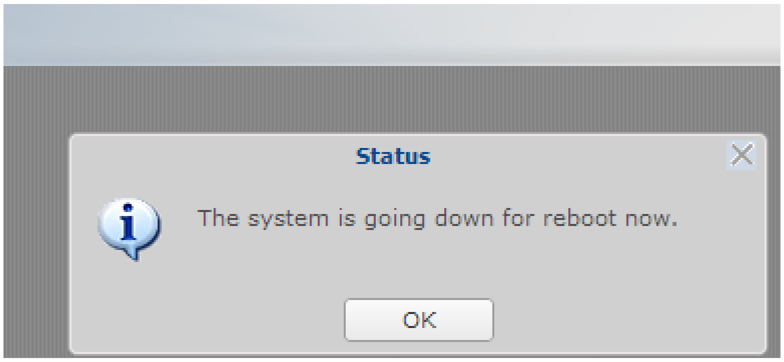


Installation is in progress. Please wait.

It takes a minimum of 20 minutes for the system software installation to complete.

7 After the software is installed Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.



The system is going down for reboot now.

If you are not able to view these messages, clear the browser cache.

8 Wait for Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

9 Verify the version in the Advanced Threat Defense web application.

10 Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

> When you upgrade to Advanced Threat Defense 3.4.8, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

11 Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of Advanced Threat Defense Appliance.

> Whitelist status is disabled after you upgrade to Advanced Threat Defense 3.4.8

Upgrade ATD software from 3.4.6 to 3.4.8

Before you begin

- Make sure that the current version of Advanced Threat Defense is 3.4.6.
- Make sure that the *system-3.4.8.msu* Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the Advanced Threat Defense web application.
- You have the credentials to log on to the Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Task

1 Log on to the Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

2 Using SFTP, upload the system-<version number>.msu file to the root directory of Advanced Threat Defense.

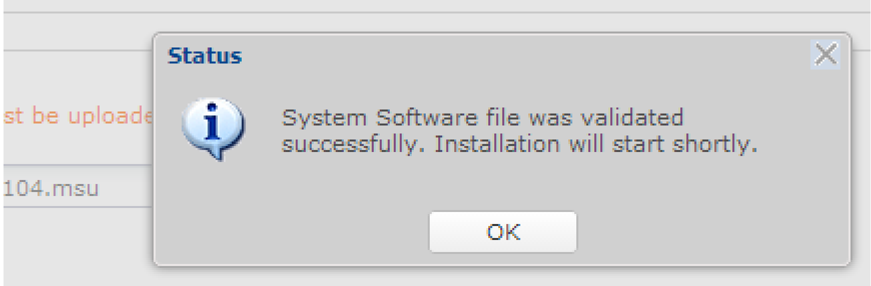
> Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

4 Under **System Software**, select the system-<version number>.msu file.

5 Make sure that **Reset Database** is deselected in case of upgrades and click **Install**.

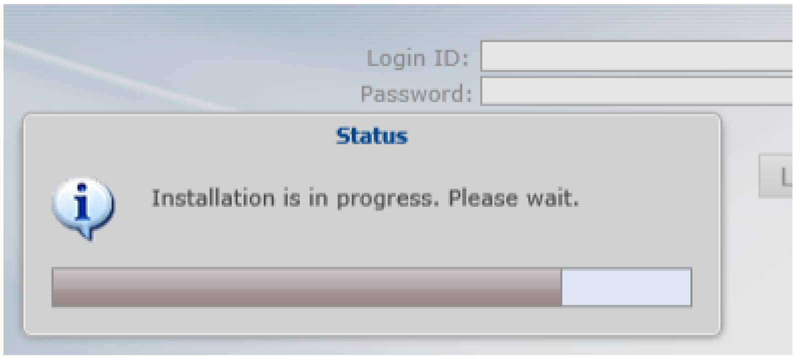
6 A confirmation message is displayed; click **OK**.



Status

System Software file was validated successfully. Installation will start shortly.

The system software is installed and the status is displayed in the browser.



Login ID:

Password:

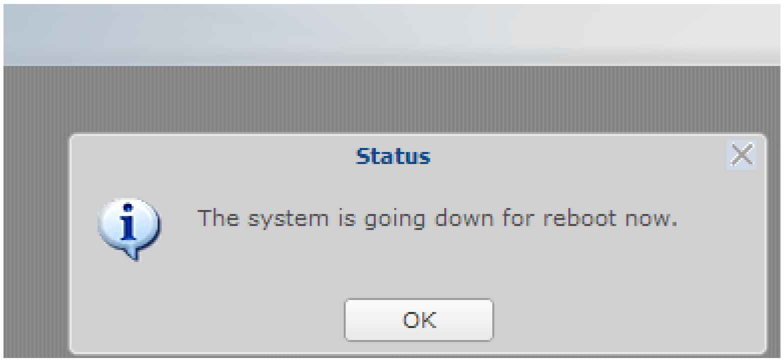
Status

Installation is in progress. Please wait.

It takes a minimum of 20 minutes for the system software installation to complete.

7 After the software is installed Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.



Status

The system is going down for reboot now.

If you are not able to view these messages, clear the browser cache.

8 Wait for Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

9 Verify the version in the Advanced Threat Defense web application.

10 Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

> When you upgrade to Advanced Threat Defense 3.4.8, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

11 Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of Advanced Threat Defense Appliance.

> Whitelist status is disabled after you upgrade to Advanced Threat Defense 3.4.8

Upgrade ATD software from 3.4.8 to higher

Before you begin

- Make sure that the current version of Advanced Threat Defense is 3.4.8.
- Make sure that the *system-3.4.8.x msu* Advanced Threat Defense software that you want to use is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the Advanced Threat Defense web application.
- You have the credentials to log on to the Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.
- LDAP configuration must be disabled before upgrading the ATD device beyond version 3.4.8.96.
- For the *atdadmin* user, the *gidNumber* value must be 1024 in the LDAP server.

Task

1 Log on to the Advanced Threat Defense Appliance using an FTP client such as FileZilla.

Log on as the atdadmin user.

2 Using SFTP, upload the system-<version number>.msu file to the root directory of Advanced Threat Defense.

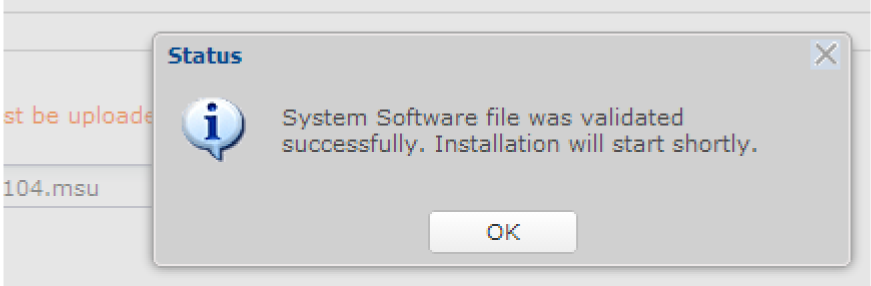
> Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

4 Under **System Software**, select the system-<version number>.msu file.

5 Make sure that **Reset Database** is deselected in case of upgrades and click **Install**.

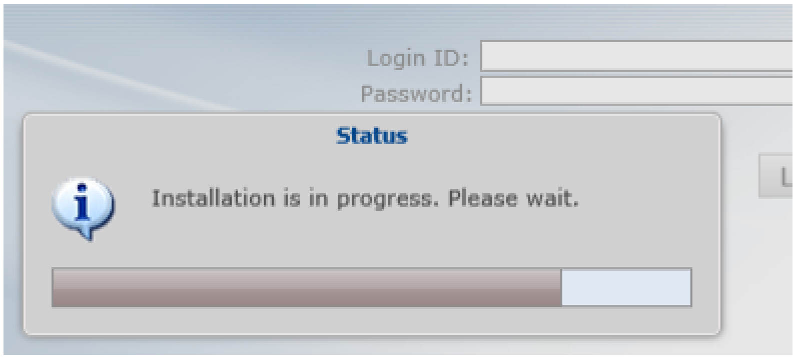
6 A confirmation message is displayed; click **OK**.



Status

System Software file was validated successfully. Installation will start shortly.

The system software is installed and the status is displayed in the browser.



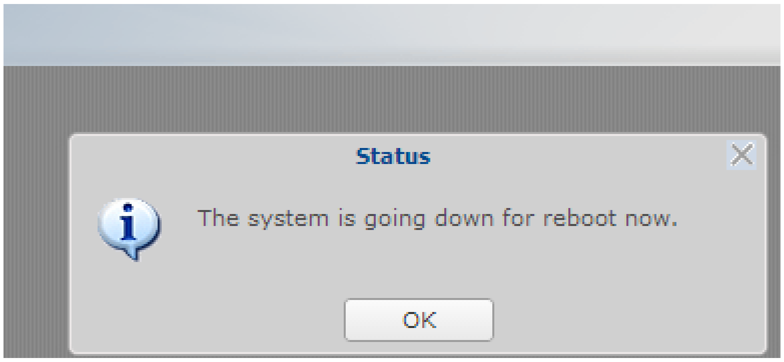
Status

Installation is in progress. Please wait.

It takes a minimum of 20 minutes for the system software installation to complete.

7 After the software is installed Advanced Threat Defense Appliance restarts. A relevant message is displayed.

The Appliance restarts on its own. The message that is displayed is only for your information.



Status

The system is going down for reboot now.

If you are not able to view these messages, clear the browser cache.

8 Wait for Advanced Threat Defense Appliance to start. Log on to the CLI and verify the software version.

9 Verify the version in the Advanced Threat Defense web application.

10 Log on to the web application, and in the **System Log** page, verify that the vmcreator task is invoked.

> When you upgrade to Advanced Threat Defense 3.4.8.x, all analyzer VMs are automatically re-created. This process might take some time to complete depending on the number of analyzer VMs.

11 Verify the data and configurations from your earlier version are preserved.

The software version you upgraded to is now stored in the active disk of Advanced Threat Defense Appliance.

> Whitelist status is disabled after you upgrade to Advanced Threat Defense 3.4.8.x.

Upgrade the Android analyzer VM

Before you begin

- Make sure that the current version of Advanced Threat Defense is 3.4.8
- Make sure that the *android-4.3.msu* is extracted and that you can access it from your client computer.
- You have the credentials to log on as the admin user in the Advanced Threat Defense web application.
- You have the credentials to log on to the Advanced Threat Defense CLI using SSH.
- You have the credentials to SFTP to the Advanced Threat Defense Appliance.
- For the *admin* user record, select **Allow Multiple Logins** in the **User Management** page.

Using the Advanced Threat Defense web application, you can upgrade the Android analyzer VM to version 4.3.

Task

1 Log on to the Advanced Threat Defense Appliance using an FTP client such as FileZilla.

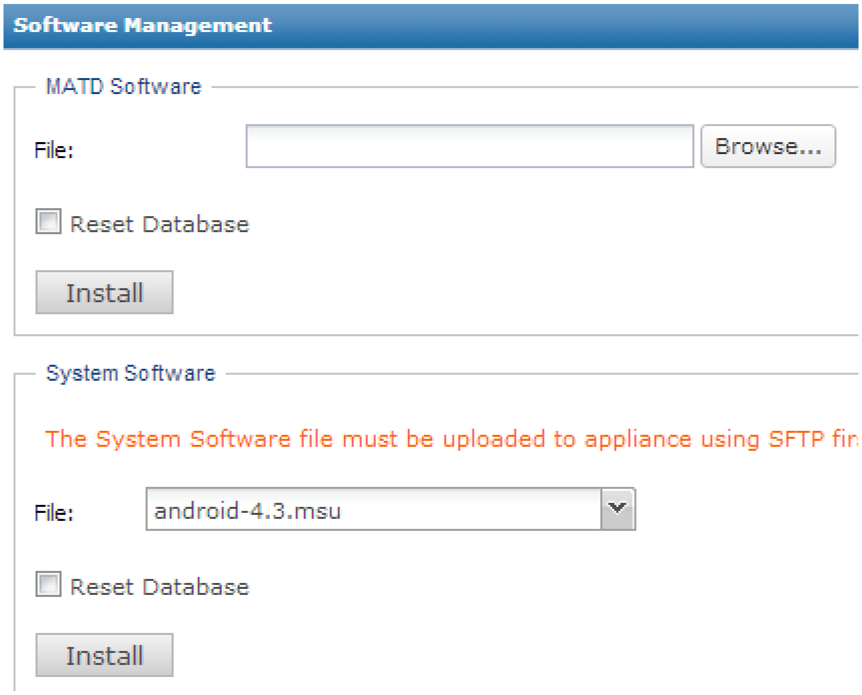
Log on as the atdadmin user.

2 Using SFTP, upload the *android-4.3.msu* file to the root directory of Advanced Threat Defense.

> Make sure that the transfer mode is binary.

3 After the file is uploaded, log on to the Advanced Threat Defense web application as the admin user and select **Manage** | **Software Management**.

4 Under **System Software**, select the *android-4.3.msu* file.



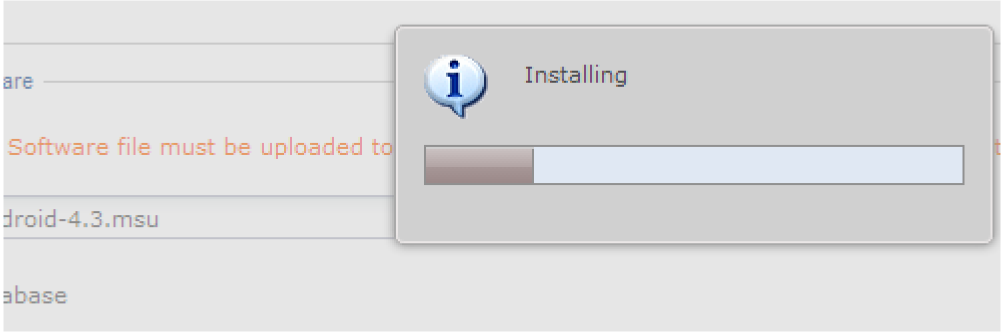
The System Software file must be uploaded to appliance using SFTP fir

File: android-4.3.msu

Figure 4-4 Select the Android file

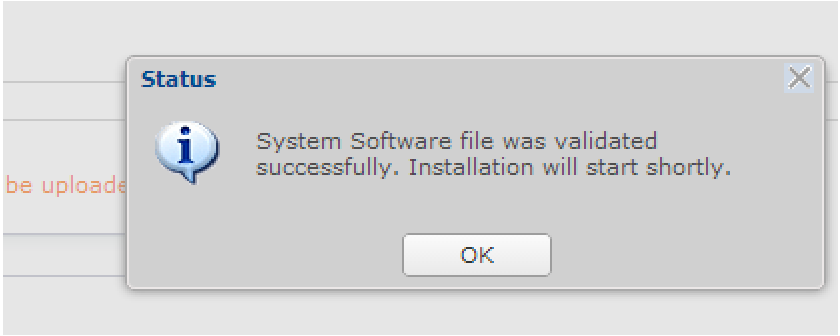
5 Make sure that **Reset Database** is deselected as this is not relevant for Android upgrade and click **Install**.

Android installation process begins with file validation.



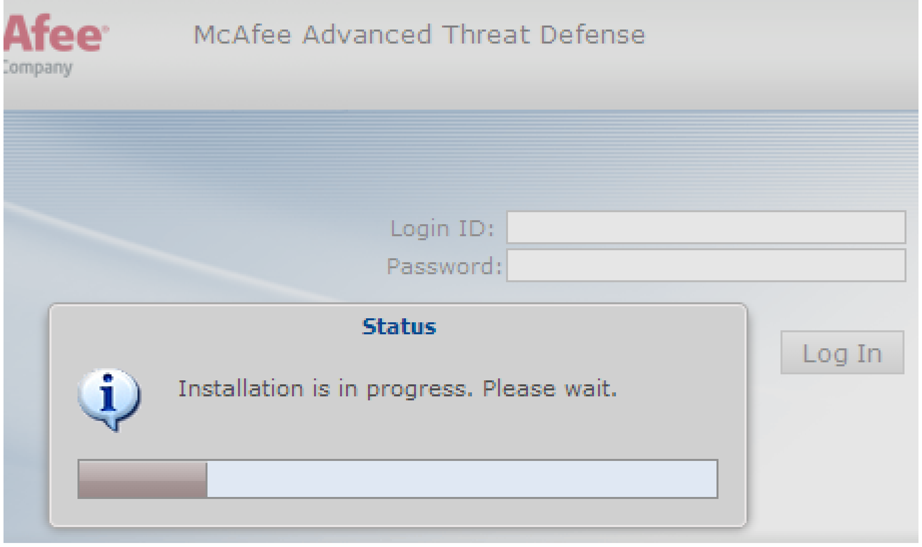
Installing

6 A confirmation message is displayed; click **OK**.



System Software file was validated successfully. Installation will start shortly.

Advanced Threat Defense web application closes logs out automatically and the status of the installation is displayed in the browser.

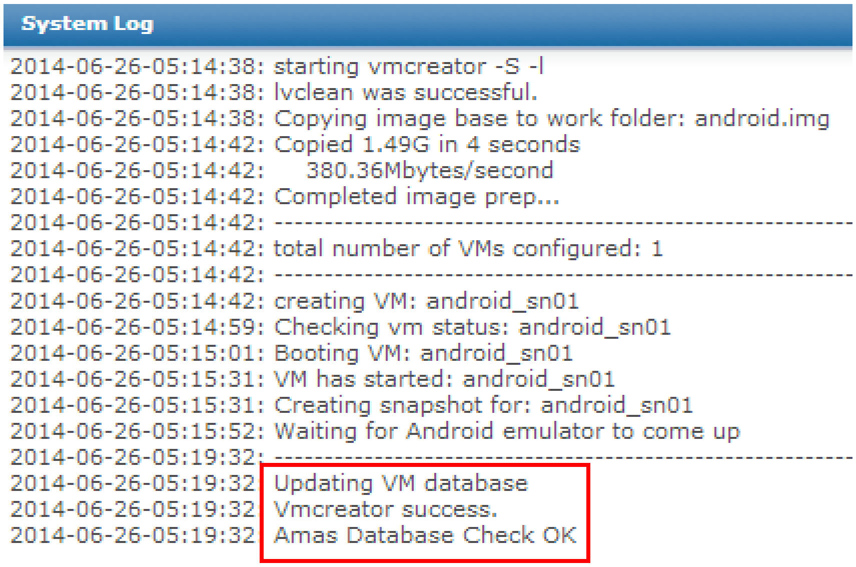


Installation is in progress. Please wait.

- It takes a minimum of 20 minutes for the system software installation to complete.
- If you are not able to view these messages, clear the browser cache.
- When you upgrade Android, the default Android analyzer VM is automatically re-created. This process might take a few minutes to complete.

7 Log on to the web application, and select **Manage** | **System Log**.

8 In the **System Log** page, verify that the vmcreator task is successfully completed for the Android analyzer VM.



```
2014-06-26-05:14:38: starting vmcreator -S -l
2014-06-26-05:14:38: lvclean was successful.
2014-06-26-05:14:38: Copying image base to work folder: android.img
2014-06-26-05:14:42: Copied 1.49G in 4 seconds
2014-06-26-05:14:42:     380.36Mbytes/second
2014-06-26-05:14:42: Completed image prep...
2014-06-26-05:14:42: -------------------------------------------------------
2014-06-26-05:14:42: total number of VMs configured: 1
2014-06-26-05:14:42: -------------------------------------------------------
2014-06-26-05:14:42: creating VM: android_sn01
2014-06-26-05:14:59: Checking vm status: android_sn01
2014-06-26-05:15:01: Booting VM: android_sn01
2014-06-26-05:15:31: VM has started: android_sn01
2014-06-26-05:15:31: Creating snapshot for: android_sn01
2014-06-26-05:15:52: Waiting for Android emulator to come up
2014-06-26-05:19:32: -------------------------------------------------------
2014-06-26-05:19:32 Updating VM database
2014-06-26-05:19:32 Vmcreator success.
2014-06-26-05:19:32 Amas Database Check OK
```

View the Upgrade log

If you want to upgrade the McAfee Advanced Threat Defense software version, you can view the upgrade path and version history logs from **Manage** | **Logs** | **Upgrade**.

The upgrade log displays details like the current software version, the previous software version, system details. Following is a sample upgrade log:

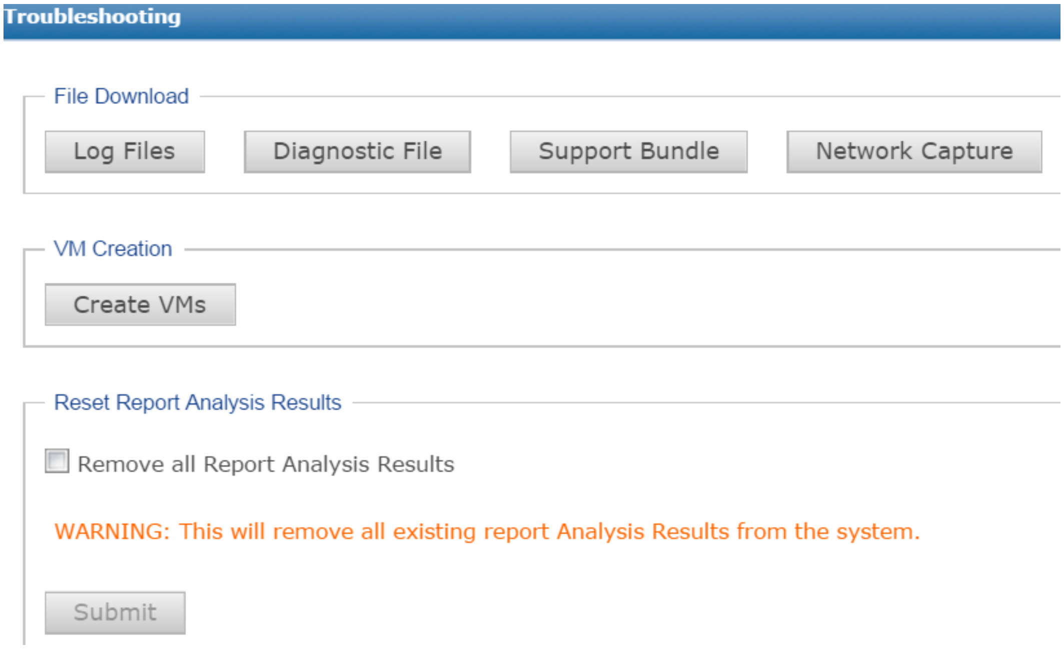
```
Tue Jul 14 02:23:12 PDT 2015 Following version of software are installed

amas build version: 3.4.8.85.50409

android build version 4.3

av-gti: release 3.4.2.32.43041

avengines: release 3.4.2.32.43041

linux-xen: release 3.4.8.82.50312

system-config: release 3.4.2.32.43041

buildscript version: : setup.sh 50362 2015-07-11 00:13:39Z <user> $

avlabS-xp-v3-3.4.8.85.50409.msi

avlabS-64-v3-3.4.8.85.50409.msi
```

Troubleshooting

The **Troubleshooting** page enables you to complete some tasks related to troubleshooting Advanced Threat Defense web application. These include exporting logs from Advanced Threat Defense, download files pertaining to Network packet capture, and clear all the stored analysis results from the Advanced Threat Defense database.

Task

1 To access the **Troubleshooting** page, select **Manage** | **Troubleshooting**.



WARNING: This will remove all existing report Analysis Results from the system.

Figure 4-5 Troubleshooting page

2 Click on **Remove all Report Analysis Results** to reset all the published analysis results from the Advanced Threat Defense.

Tasks

- *Export Advanced Threat Defense logs* on page 56
- *Recreate the analyzer VMs* on page 57
- *Delete the analysis results* on page 58

Export Advanced Threat Defense logs

If you face issues using Advanced Threat Defense, you can export the log files and provide them to McAfee support for analysis and troubleshooting. You can export system logs, diagnostic logs, and additional miscellaneous logs. The system logs help to troubleshoot issues related to features, operations, events, and so on. The diagnostic logs are needed to troubleshoot critical issues such as system crashes in Advanced Threat Defense.

> You cannot read the contents of system or diagnostic log files. All these logs are intended for McAfee support.

Task

1 In the **Troubleshooting** page, click **Log files** to download the system logs and **Diagnostic File** to download the diagnostic logs.

2 To download the network packet capture file, click **Network Capture**. The network capture action stops automatically once the file size reaches 10 megabyte.

3 To download the additional miscellaneous information and logs, click **Support Bundle**, enter the ticket number, and click **OK**.

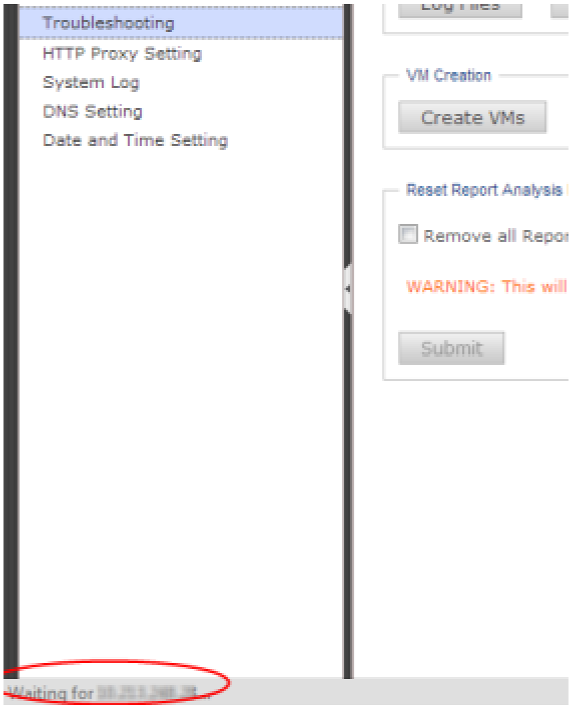


Figure 4-6 Support bundle creation

Advanced Threat Defense collects the required information and a message is displayed at the bottom of the browser. After some time, option to save the <ticket number>.tgz file is provided.

4 Provide the following files to McAfee support.

- System logs (atdlogs.bin)
- Diagnostic logs (atdcore.bin)
- Additional miscellaneous logs (<ticket number>.tgz)

Recreate the analyzer VMs

During dynamic analysis, samples might corrupt some of the analyzer VMs. So, these analyzer VM instances might not be available for further analysis. Under such circumstances, you can delete all the existing analyzer VMs and recreate them.

All the existing analyzer VMs including the default Android VM and also the healthy analyzer VMs are deleted and re-created. So, no file analysis is possible until all the analyzer VMs are created again. The time taken for the re-creation varies based on the number of analyzer VM instances as well as their size.

If you re-activate Windows license on the VMDK by VNC connection, you need to update these changes onto the existing analyzer VM instances. Under such circumstances, you can also delete the target VM profile and create a new VM profile.

Task

1. In the **Troubleshooting** page, click **Create VMs** and confirm that you want to delete all existing analyzer VM instances and recreate them.
2. Select **Manage** | **Logs** | **System** to view the logs related to VM re-creation.

   You can select **Dashboard** and view the **VM Creation Status** monitor to know the progress of VM re-creation. The **Create VMs** button in the **Troubleshooting** page is available again only after all the analyzer VM instances have been re-created.

Delete the analysis results

Task

1. In the **Troubleshooting** page, click **Remove all Report Analysis Results**.

   > Once we click **Remove all Report Analysis Results**, all blacklist entries, whether added manually or added automatically are flushed.

2. Click **Submit.**

Back up and restore the Advanced Threat Defense database

As a precaution, you can periodically backup the Advanced Threat Defense database. You can then restore a backup of your choice when required. For example, if you want to discard all changes made during a troubleshooting exercise, you can restore the backup that was taken before you started troubleshooting.

You can schedule automatic backups to a designated FTP server on a daily, weekly, or monthly basis.

When you want to restore a backup, Advanced Threat Defense fetches the selected backup file from the FTP server and overwrites its database with the contents of the backup file.

What gets backed up?

The following data gets backed up:

- Results as displayed in the **Analysis Results** page

  > Analysis reports such as the analysis summary, complete results, and disassembly results are not backed up. If you delete the reports from the database (from the **Troubleshooting page**) and then restore a backup, the detailed result is listed in the **Analysis Results** page from the backup, but the reports are not available.

- Local blacklist (local whitelist is not backed up)
- VM profiles

  > The image or VMDK file of the analyzer VMs are not backed up. Before you restore a backup, make sure the image files specified in the backed-up VM profiles are present in McAfee Advanced Threat Defense.

- Analyzer profiles
- User records
- McAfee ePO integration details

- Proxy settings
- DNS settings
- Syslog settings
- SNMP settings
- Date and time settings including the NTP server details
- Load-balancing cluster settings as displayed in the **Load Balancing Cluster Setting** page

  This does not include the configuration and analysis results from the other nodes in the cluster.

- Custom YARA rules and configuration
- Backup scheduler settings
- Backed-up file details as displayed in the **Restore Management** page

The following data does not get backed up:

- Any sample file or URL that is being analyzed at the time of backup

  The **Analysis Status** page only shows the file being currently analyzed

- The VMDK or image files of analyzer VMs
- The Advanced Threat Defense software in the active or backup disk
- The log files and diagnostic files
- The information pertaining to the network in which the Advanced Threat Defense Appliance is present. That is appliance IP, subnet mask, gateway, appliance name (if any) and so on.

Schedule a database backup

You can schedule automatic backups on a daily, weekly, or monthly frequency. The time taken for the backup process to complete is usually a few minutes. However, it varies based on the size of the data involved. McAfee recommends that you choose a time when the analysis load on the Advanced Threat Defense is likely to be less.

Before you begin

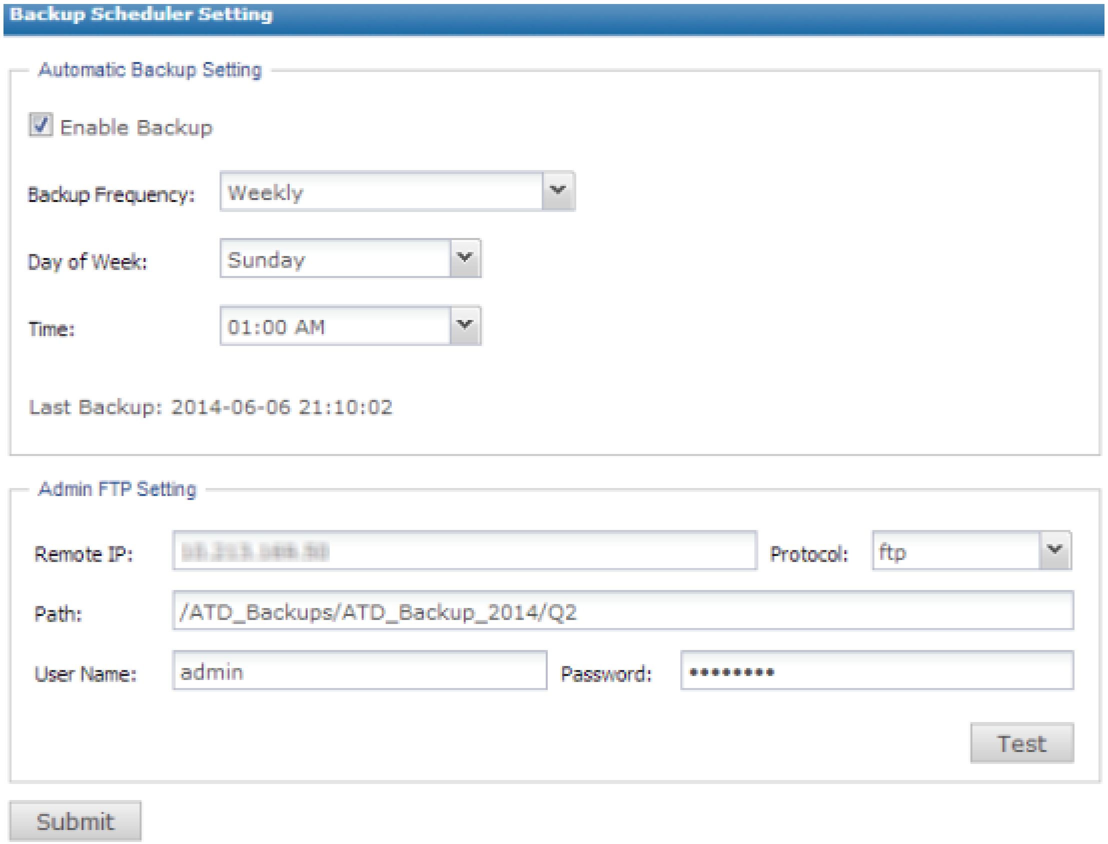
- You must be the admin user in Advanced Threat Defense web application.
- You must have a configured FTP server for storing the backups and you are aware of the directory in which you want to store the backups.
- You must have the IPv4 address of the FTP server, the user name, and the password for Advanced Threat Defense to access that FTP server. A password can contain only following special characters ` ~ ! @ # $ % ^ & *. Also, the user name has write access to the directory that you plan to use.
- Communication over SFTP or FTP must be possible between Advanced Threat Defense and the FTP server.

Because the backup feature is configurable for the admin user only, the FTP server settings in the **Backup Scheduler Setting** page and the **FTP Result Output** settings on the **User Management** page for the admin user are the same. So, when the administrator user modifies the FTP details on one of those pages, it automatically reflects on the other page.

Task

1 Select **Manage** | **Restore & Backup** | **Backup.**

The **Backup Scheduler Setting** page is displayed.



Backup Scheduler Setting

Automatic Backup Setting

☑ Enable Backup

Backup Frequency: Weekly

Day of Week: Sunday

Time: 01:00 AM

Last Backup: 2014-06-06 21:10:02

Admin FTP Setting

Remote IP: [redacted] Protocol: ftp

Path: /ATD_Backups/ATD_Backup_2014/Q2

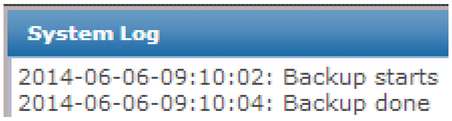
User Name: admin Password: •••••••••

Figure 4-7 Schedule a backup

2 Enter the appropriate information in the respective fields.

Option name	Definition
Enable Backup	Select to enable automatic backup at the scheduled time. If you want to stop the automatic backup, deselect this checkbox.
Backup Frequency	Specify how frequently you want Advanced Threat Defense to back up the database. - **Daily** — Select to back up daily. **Time** — Specify the time for the daily backup. For example, if you select 1 a.m, Advanced Threat Defense backs up at 1 a.m. daily according to its clock. To back up immediately, you can use the `show` command on the Advanced Threat Defense CLI to know the current time on Advanced Threat Defense. Then with **Daily** as the backup frequency, you can specify a time accordingly to back up immediately. - **Weekly** — Select to back-up once a week. - **Day of the week** — Select the day when you want to back up. - **Time** — Specify the time of the backup on the selected day. - **Monthly** — Select to backup once a month. - **Day of Month** — Select the date when you want to back up. For example, if you select 5, Advanced Threat Defense backs up the database on the fifth of every month. You can only specify a date up to 28. This avoids invalid dates such as February 30. - **Time** — Specify the time of the backup on the selected date.
Last Backup	Time stamp of the last successful backup.
Remote IP	The IPv4 address of the FTP server.
Protocol	Select if you want Advanced Threat Defense to use FTP or SFTP to transfer the backup file to the FTP server.
Path	The directory where Advanced Threat Defense must save the file on the FTP server. For example, to save the file at the root directory, enter the directory, enter:/.
User Name	The user name that Advanced Threat Defense must use to access the FTP server. Make sure that this user name has write access to the specified folder.
Password	The corresponding password. A password can contain only following special characters ` ~ ! @ # $ % ^ & *
Test	Click to make sure that Advanced Threat Defense is able to access the specified FTP server using the selected protocol and user credentials. You can schedule a backup successfully only if the test connection succeeds.
Submit	Click to schedule the backup.

3. To view the logs related to backup, select **Manage** | **Logs** | **Syslog** to view the details such as the start and end time stamps.



System Log

```
2014-06-06-09:10:02: Backup starts
2014-06-06-09:10:04: Backup done
```

Figure 4-8 Logs related to backup

The backup is stored in a password-protected .zip file in the specified directory in the FTP server.

> Do not try to unzip or tamper with this file. If the file gets corrupted, you might not be able to restore the database backup using that file.

Restore a database backup - Specific backup file

Before you begin

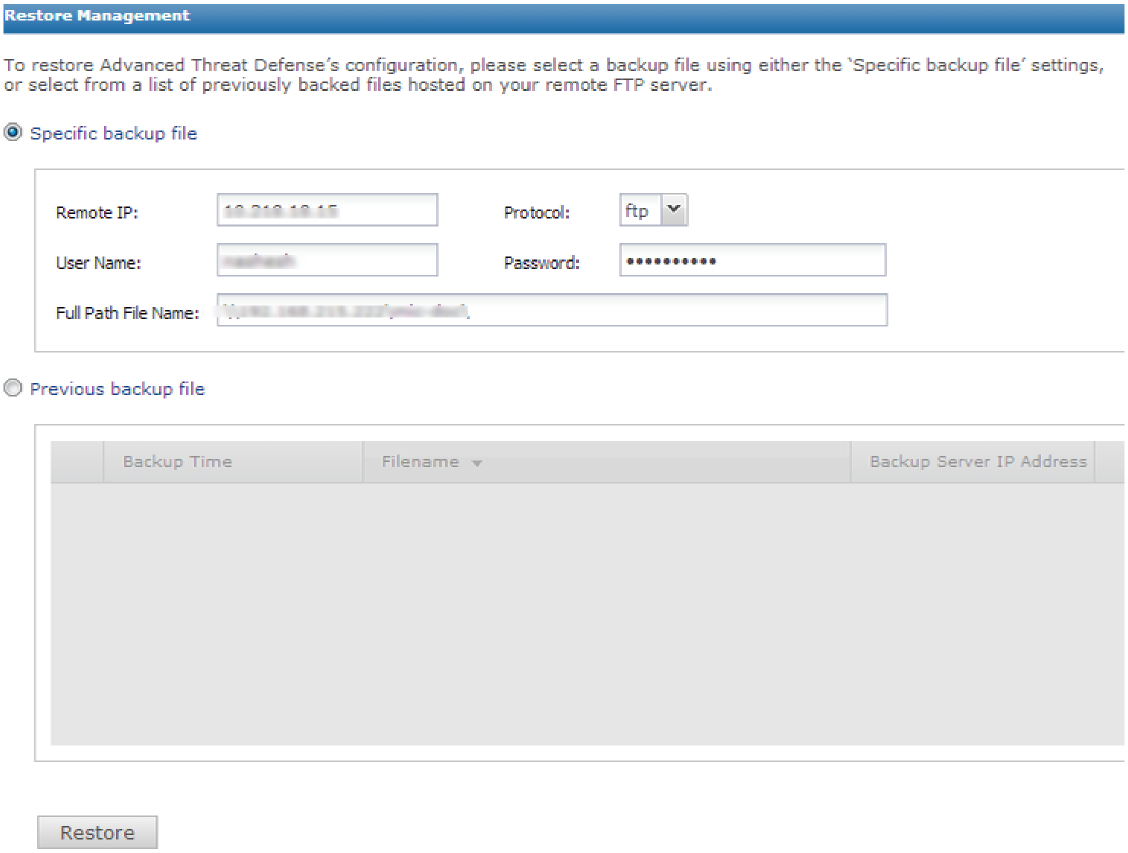
- Make sure that you configured the FTP IP address, directory path, and user credentials on the **Backup Scheduler Setting** page and the test connection is working for the specified configuration. You can restore a backup only from the same FTP server that you used for taking the backup.
- Make sure that the corresponding backup file that you plan to restore is available on the FTP server at the specified directory.
- As a precaution, make sure that there is no other user logged on to Advanced Threat Defense during the restoration window. Factor in the Advanced Threat Defense web application, REST APIs, and CLI.
- Make sure that Advanced Threat Defense is not analyzing any sample files or URLs at the time of restoration. Also, make sure no integrated product, user, or script is submitting samples during the restoration window.
- Make sure that you do not restore a backup during the backup window.
- Make sure that there is no Advanced Threat Defense software upgrade happening during the restoration window.

Using **Specific backup file**, you can restore the backup file that is present in the FTP server to any Advanced Threat Defense appliance. This is useful when the Advanced Threat Defense appliance gets corrupted.

> You cannot restore a backup from an earlier or later version of Advanced Threat Defense software. All numbers in the version must exactly match. For example, you cannot restore a backup from 3.0.4.94.39030 on 3.0.4.94.39031.

Task

1 Select **Manage** | **Restore & Backup** | **Restore**



Restore Management

To restore Advanced Threat Defense's configuration, please select a backup file using either the 'Specific backup file' settings, or select from a list of previously backed files hosted on your remote FTP server.

● Specific backup file

Remote IP: [redacted] Protocol: ftp

User Name: [redacted] Password: •••••••••••

Full Path File Name: [redacted]

○ Previous backup file

	Backup Time	Filename	Backup Server IP Address

Figure 4-9 Specific backup file

2 Select **Specific backup file**. Enter the appropriate information in the respective fields.

Table 4-1 Restore a specific backup file

Option name	Definition
Remote IP	The IPv4 address of the FTP server.
Protocol	Select if you want the Advanced Threat Defense to use FTP or SFTP to transfer the backup file to the FTP server.
User Name	The user name that Advanced Threat Defense must use to access the FTP server. Make sure that this user name has write access to the specified folder.
Password	The corresponding password.
Full Path File Name	Complete location of previously created file and file name must be given in order to restore the backup. Restoration fails if the backup file is not available at the specified location on the backup server.

3 Click **Restore**.

Restore a database backup - Previous backup file

Before you begin

- Make sure that you configured the FTP IP address, directory path, and user credentials on the **Backup Scheduler Setting** page and the test connection is working for the specified configuration. You can restore a backup only from the same FTP server that you used for taking the backup.
- Make sure that the corresponding backup file that you plan to restore is available on the FTP server at the specified directory.
- As a precaution, make sure that there is no other user logged on to Advanced Threat Defense during the restoration window. Factor in the Advanced Threat Defense web application, REST APIs, and CLI.
- Make sure that Advanced Threat Defense is not analyzing any sample files or URLs at the time of restoration. Also, make sure no integrated product, user, or script is submitting samples during the restoration window.
- Make sure that you do not restore a backup during the backup window.
- Make sure that there is no Advanced Threat Defense software upgrade happening during the restoration window.

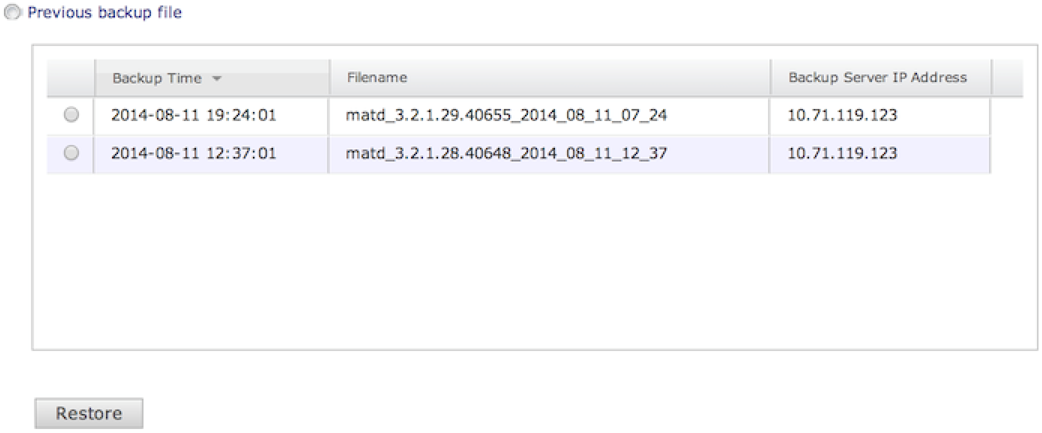
There might be some changes regarding the FTP server used for the backup. For example, the IP address of the FTP backup server might change or you might want to migrate the FTP server to a new physical or virtual server. If the IP address changes, make sure you update the configuration accordingly on the **Backup Scheduler Setting** page. You can then restore from the required backup file. However, if the server itself is changed, you cannot restore the backups stored on the old server. You can only restore from the files backed up on the new server.

- You cannot restore a backup from an earlier or later version of Advanced Threat Defense software. All numbers in the version must exactly match. For example, you cannot restore a backup from 3.0.4.94.39030 on 3.0.4.94.39031.
- The time taken for the backup restore process to complete is usually a few minutes. However, it varies based on the size of the data involved.

Task

1 Select **Manage** | **Backup and Restore** | **Restore**

The **Restore Management** page is displayed.



○ Previous backup file

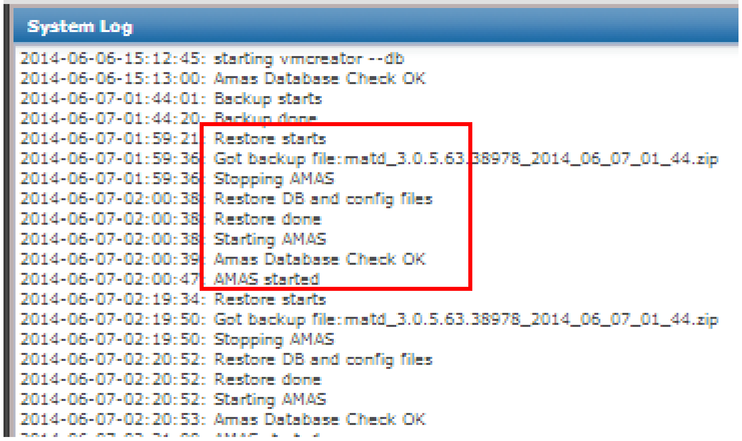
	Backup Time	Filename	Backup Server IP Address
○	2014-08-11 19:24:01	matd_3.2.1.29.40655_2014_08_11_07_24	10.71.119.123
○	2014-08-11 12:37:01	matd_3.2.1.28.40648_2014_08_11_12_37	10.71.119.123

Figure 4-10 List of available backup files

Table 4-2 Restore previous backup files

Option name	Definition
File Name	The name, which Advanced Threat Defense assigned to the backup file. ℹ Do not attempt to change the file name in the FTP server.
Backup Server IP Address	The IP address of the FTP server in which the backup files are stored.
Backup Time	Time stamp of when the backup was taken.
Restore	Select the required backup file and click **Restore** to restore the data from that backup file. When you have more than one backup file, you can select the backup files that you want to restore using the radio buttons.

2 To view the logs related to restore, select **Manage** | **Logs** | **Syslog**.



System Log

```
2014-06-06-15:12:45: starting vmcreator --db
2014-06-06-15:13:00: Amas Database Check OK
2014-06-07-01:44:01: Backup starts
2014-06-07-01:44:20: Backup done
2014-06-07-01:59:21: Restore starts
2014-06-07-01:59:36: Got backup file:matd_3.0.5.63.38978_2014_06_07_01_44.zip
2014-06-07-01:59:36: Stopping AMAS
2014-06-07-02:00:38: Restore DB and config files
2014-06-07-02:00:38: Restore done
2014-06-07-02:00:38: Starting AMAS
2014-06-07-02:00:39: Amas Database Check OK
2014-06-07-02:00:47: AMAS started
2014-06-07-02:19:34: Restore starts
2014-06-07-02:19:50: Got backup file:matd_3.0.5.63.38978_2014_06_07_01_44.zip
2014-06-07-02:19:50: Stopping AMAS
2014-06-07-02:20:52: Restore DB and config files
2014-06-07-02:20:52: Restore done
2014-06-07-02:20:52: Starting AMAS
2014-06-07-02:20:53: Amas Database Check OK
```

Figure 4-11 Logs related to data restore

The processes related to sample analysis are stopped before the restore process and restarted after the restore process.

5 Creating analyzer VM

For dynamic analysis, Advanced Threat Defense executes a suspicious file in a secure virtual machine (VM) and monitors its behavior for malicious activities. This VM is referred to as an analyzer VM. This chapter provides the steps for creating an analyzer VM and the VM profile.

> Any security software or low-level utility tool on an analyzer VM, might interfere with the dynamic analysis of the sample file. The sample-file execution might itself be terminated during dynamic analysis. As a result, the reports might not capture the full behavior of the sample file. If you need to find out the complete behavior of a sample file, do not patch the operating system of the analyzer VM or install any security software on it. If you need to find out the effect of the sample file specific to your network, use your Common Operating Environment (COE) image, with the regular security software, to create the analyzer VMs.

The high-level steps for creating an analyzer VM and the VM profile are as follows:

1. Create an ISO image of the corresponding operating system. You must also have the license key for that operating system. For example, to create an Windows 7 analyzer VM, you must have an ISO image of Windows 7 and the license key.

   Only the following operating systems are supported to create the analyzer VMs:

   - Microsoft Windows XP 32-bit Service Pack 2
   - Microsoft Windows XP 32-bit Service Pack 3
   - Microsoft Windows Server 2003 32-bit Service Pack 1
   - Microsoft Windows Server 2003 32-bit Service Pack 2
   - Microsoft Windows Server 2008 R2 Service Pack 1
   - Microsoft Windows 7 32-bit Service Pack 1
   - Microsoft Windows 7 64-bit Service Pack 1
   - Microsoft Windows 8.0 Pro 32-bit
   - Microsoft Windows 8.0 Pro 64-bit
   - Android 2.3 by default. You can upgrade it to Android 4.3. See Upgrade the Android analyzer VM on page 52.

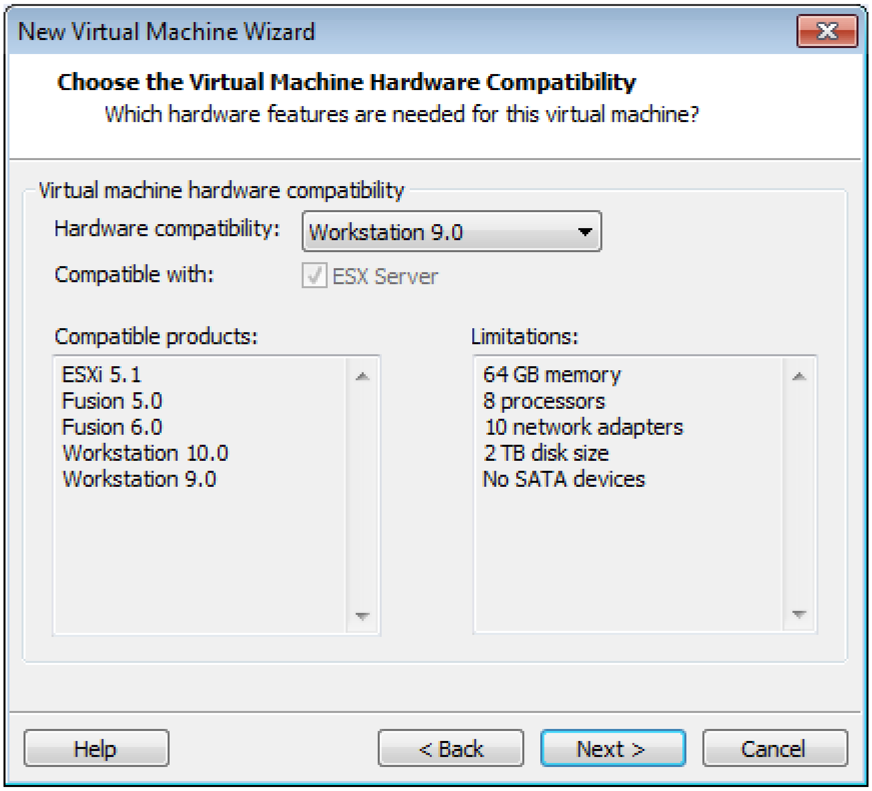
   All of the above Windows operating systems can be in English, Chinese Simplified, Japanese, German, or Italian.

   > The only pre-installed analyzer VM is the Android VM.

2 Using VMware Workstation 9.0, create a Virtual Machine Disk (VMDK) file of the ISO image. After you create the VM, you can install the required applications such as:

- Internet Explorer versions 6, 7, 8, 9, and 10
- Mozilla Firefox versions 11, 12, and 13
- Microsoft Office versions 2003, 2007, 2010, and 2013
- Adobe Reader version 9, 10 and 11

Recommended VMware workstation version is 9.0. However, if you use VMware Workstation 10.0 or VMware Workstation 11.0, select **Workstation 9.0** under **Hardware Compatibility** in **New Virtual Machine Wizard** as shown below:


New Virtual Machine Wizard

Choose the Virtual Machine Hardware Compatibility

Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware compatibility: Workstation 9.0

Compatible with: ☑ ESX Server

Compatible products:
ESXi 5.1
Fusion 5.0
Fusion 6.0
Workstation 10.0
Workstation 9.0

Limitations:
64 GB memory
8 processors
10 network adapters
2 TB disk size
No SATA devices

3 Import the VMDK file into the Advanced Threat Defense Appliance.

4 Convert the VMDK file into an image (.img) file.

5 Create the VM and the VM profile.

If you already have a VMDK file, it must be a single file that contains all the files required to create the VM.

The following table specifies the maximum number of VMs that can be created based on different Windows flavor.

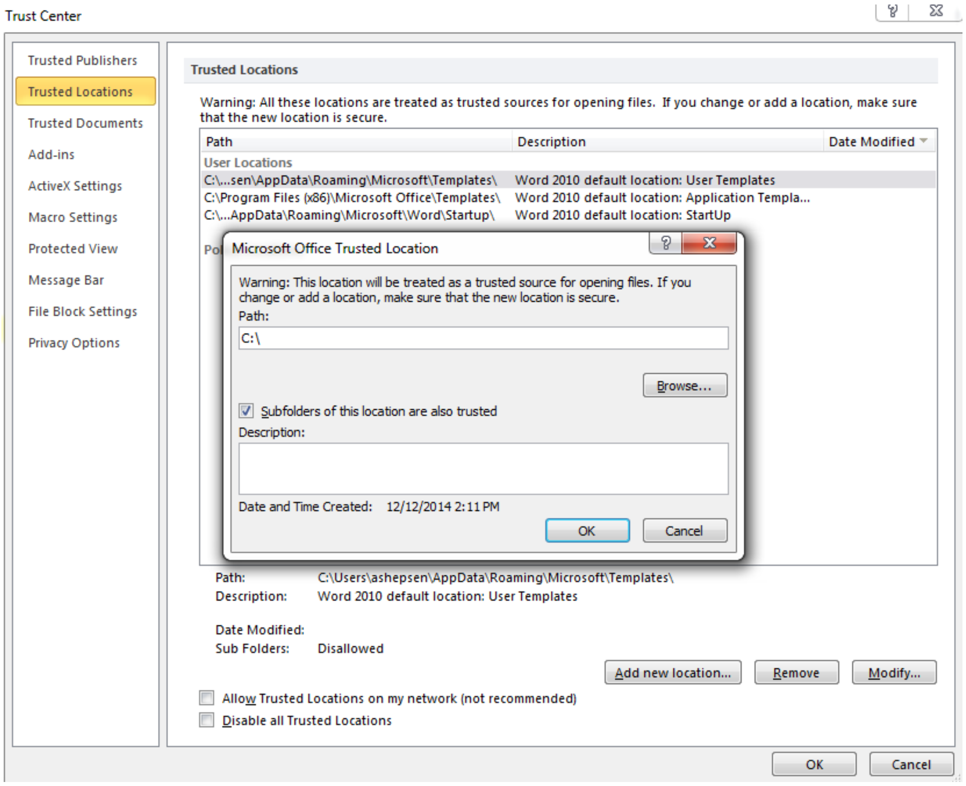
Table 5-1 Number of VMs per OS

OS (Windows Platform)	ATD-3000 (Number of VMs)	ATD-6000 (Number of VMs)
WinXP SP2 (5 GB)	29	59
WinXP SP3 (5 GB)	29	59
Windows 2003 SP1 (5 GB)	29	59
Windows 2003 SP2 (5 GB)	29	59
Windows 2008 64bit SP1 (14 GB)	29	59
Windows 7 32bit (14 GB)	29	59
Windows 7 64bit (14 GB)	29	59
Windows 8 32bit (24 GB)	29	59
Windows 8 64bit (24 GB)	29	59

Android VM is default with all Advanced Threat Defense Appliance installations. Also, the Windows platforms listed in the table above shows hard disk space occupied in the base/default form, if you wish install updates and patches, then you must chose your OS keeping the hard disk space constraint in mind.

Below is the Microsoft Office setting that needs to be enabled after installing Microsoft Office versions 2003, 2007, 2010, or 2013. The below steps enable Auto Macros functionality in Microsoft Office:

1 Under **<Microsoft Office Application>** | **File** | **Option** | **Trust Center** | **Trusted Locations**, select the desired **Path** under **User Locations**, click on **Subfolders of this location are also trusted** and click **OK**.



Trusted Locations

Warning: All these locations are treated as trusted sources for opening files. If you change or add a location, make sure that the new location is secure.

Path	Description	Date Modified
User Locations		
C:\...sen\AppData\Roaming\Microsoft\Templates\	Word 2010 default location: User Templates	
C:\Program Files (x86)\Microsoft Office\Templates\	Word 2010 default location: Application Templa...	
C:\...AppData\Roaming\Microsoft\Word\Startup\	Word 2010 default location: StartUp	

Microsoft Office Trusted Location

Warning: This location will be treated as a trusted source for opening files. If you change or add a location, make sure that the new location is secure.

Path: C:\

Browse...

☑ Subfolders of this location are also trusted

Description:

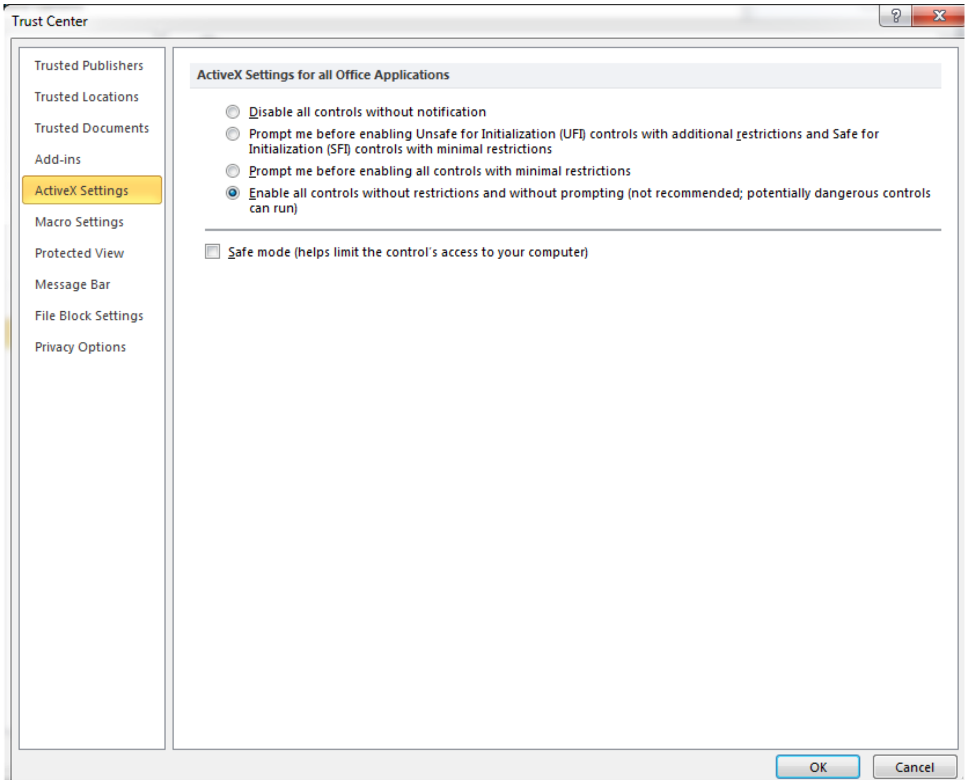
Date and Time Created: 12/12/2014 2:11 PM

OK Cancel

Path: C:\Users\ashepsen\AppData\Roaming\Microsoft\Templates\
Description: Word 2010 default location: User Templates
Date Modified:
Sub Folders: Disallowed

☐ Allow Trusted Locations on my network (not recommended)
☐ Disable all Trusted Locations

2 Under **<Office Application>** | **File** | **Option** | **Trust Center** | **ActiveX Settings**, select **Enable all controls without restrictions and without prompting** and click **OK**.



ActiveX Settings for all Office Applications

○ Disable all controls without notification

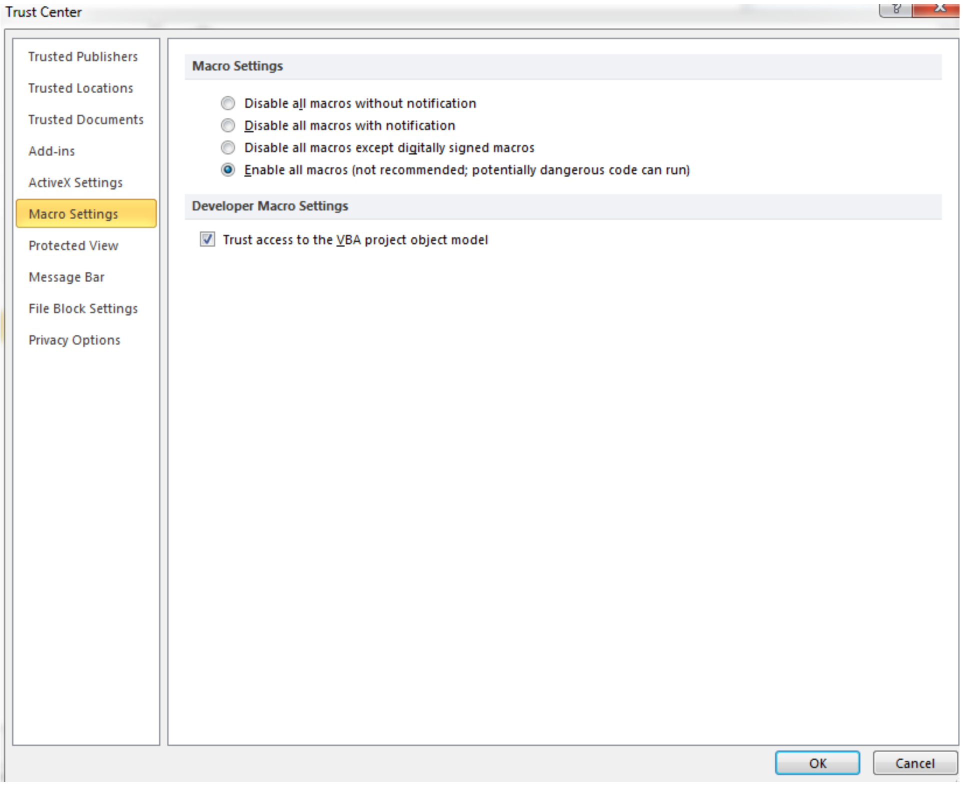
○ Prompt me before enabling Unsafe for Initialization (UFI) controls with additional restrictions and Safe for Initialization (SFI) controls with minimal restrictions

○ Prompt me before enabling all controls with minimal restrictions

● Enable all controls without restrictions and without prompting (not recommended; potentially dangerous controls can run)

□ Safe mode (helps limit the control's access to your computer)

3 Under **<Office Application>** | **File** | **Option** | **Trust Center** | **Macro Settings**, select **Enable all macros** and click **OK**.



Macro Settings

○ Disable all macros without notification

○ Disable all macros with notification

○ Disable all macros except digitally signed macros

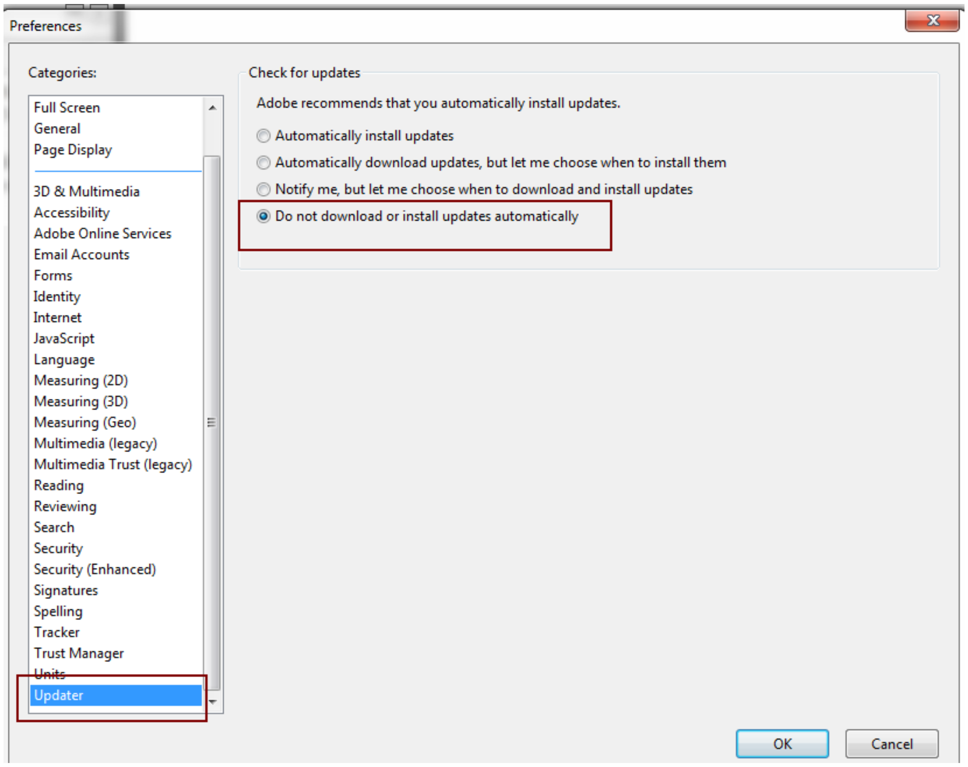
● Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

☑ Trust access to the VBA project object model

Below is the Adobe Reader setting that needs to be selected after installing Adobe Reader version 8, 9, or 10:

1 Under **Adobe Reader** | **Preferences** | **Updater**, select **Do not download or install updates automatically** and click **OK**.



Preferences

Check for updates

Adobe recommends that you automatically install updates.

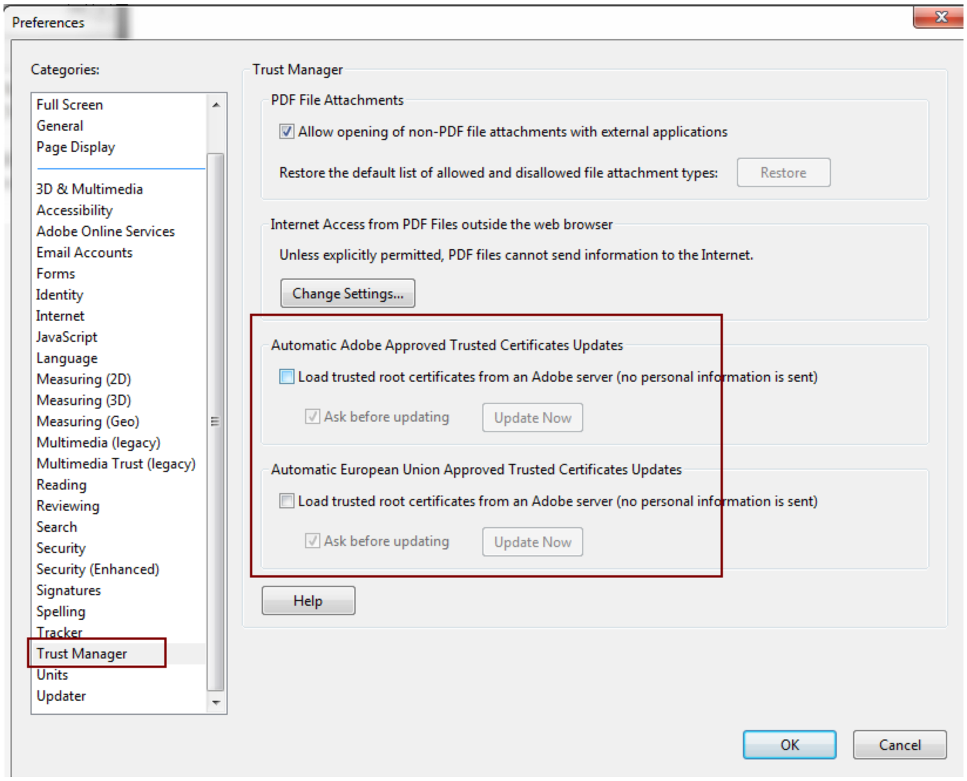
○ Automatically install updates

○ Automatically download updates, but let me choose when to install them

○ Notify me, but let me choose when to download and install updates

● Do not download or install updates automatically

2 Under **Adobe Reader** | **Preferences** | **Trust Manager**, select **Ask before updating** in **Automatic Adobe Approved Trusted Certificates Updates** section and click **OK**.



Trust Manager

PDF File Attachments

☑ Allow opening of non-PDF file attachments with external applications

Restore the default list of allowed and disallowed file attachment types:

Internet Access from PDF Files outside the web browser

Unless explicitly permitted, PDF files cannot send information to the Internet.

Automatic Adobe Approved Trusted Certificates Updates

□ Load trusted root certificates from an Adobe server (no personal information is sent)

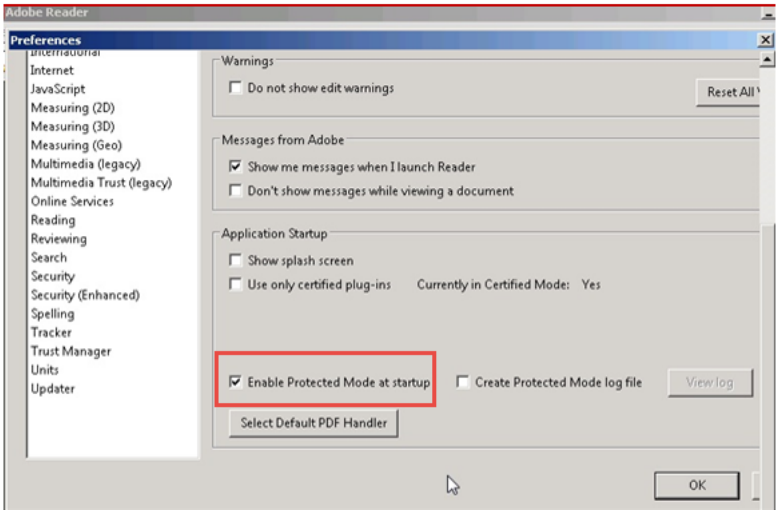
☑ Ask before updating

Automatic European Union Approved Trusted Certificates Updates

□ Load trusted root certificates from an Adobe server (no personal information is sent)

☑ Ask before updating

3 Under **Adobe Reader** | **Preferences** | **General**, select **Enable Protected Mode at startup** and click **OK**.



Warnings

□ Do not show edit warnings

Messages from Adobe

☑ Show me messages when I launch Reader

□ Don't show messages while viewing a document

Application Startup

□ Show splash screen

□ Use only certified plug-ins Currently in Certified Mode: Yes

☑ Enable Protected Mode at startup □ Create Protected Mode log file

Contents

- *Create a VMDK file for Windows XP*
- *Create a VMDK file for Windows 2003 Server*
- *Create a VMDK file for Windows 7*
- *Create a VMDK file for Windows 2008 Server*
- *Create a VMDK file for Windows 8*
- *Import a VMDK file into Advanced Threat Defense*
- *Convert the VMDK file to an image file*

- *Managing VM profiles*
- *View the System log*

Create a VMDK file for Windows XP

Before you begin

- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure you have the ISO image of Windows XP SP2 or SP3 operating system for which you need to create the VMDK file. Only Windows Professional is supported.
- Make sure you have the license key for the operating system.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image.

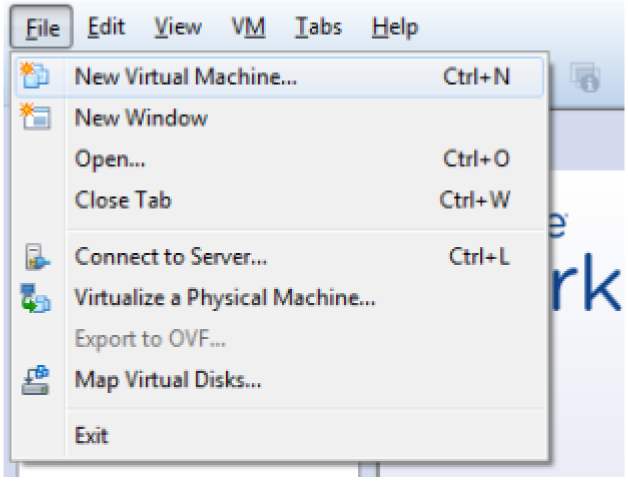
Step	Details
Step 1: Start the VMware Workstation.	This procedure uses VMware Workstation 10 as an example.
Step 2: In the VMware Workstation page, select **File | New Virtual Machine.**	 File Edit View VM Tabs Help New Virtual Machine... Ctrl+N New Window Open... Ctrl+O Close Tab Ctrl+W Connect to Server... Ctrl+L Virtualize a Physical Machine... Export to OVF... Map Virtual Disks... Exit

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

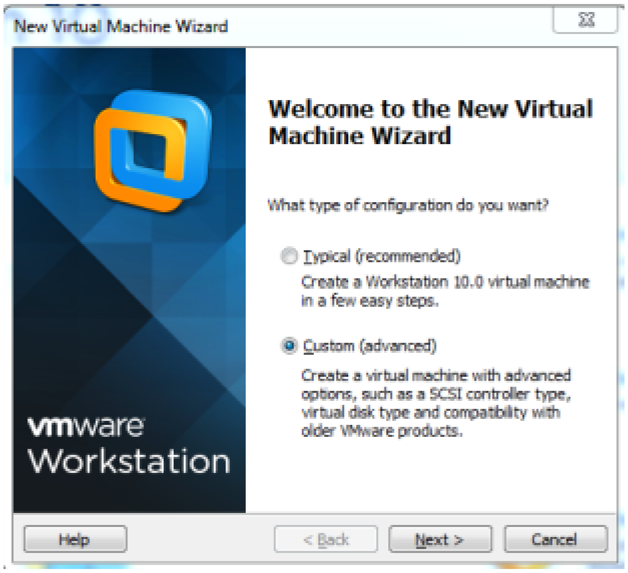
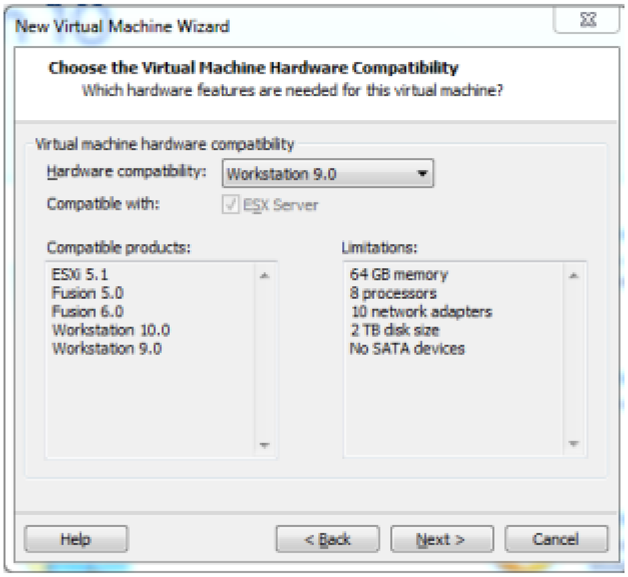
Step	Details
Step 3: In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.**	 New Virtual Machine Wizard Welcome to the New Virtual Machine Wizard What type of configuration do you want? ○ Typical (recommended) Create a Workstation 10.0 virtual machine in a few easy steps. ● Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Step 4: In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next.**	 New Virtual Machine Wizard Choose the Virtual Machine Hardware Compatibility Which hardware features are needed for this virtual machine? Virtual machine hardware compatibility Hardware compatibility: Workstation 9.0 Compatible with: ☑ ESX Server Compatible products: ESXi 5.1 Fusion 5.0 Fusion 6.0 Workstation 10.0 Workstation 9.0 Limitations: 64 GB memory 8 processors 10 network adapters 2 TB disk size No SATA devices

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

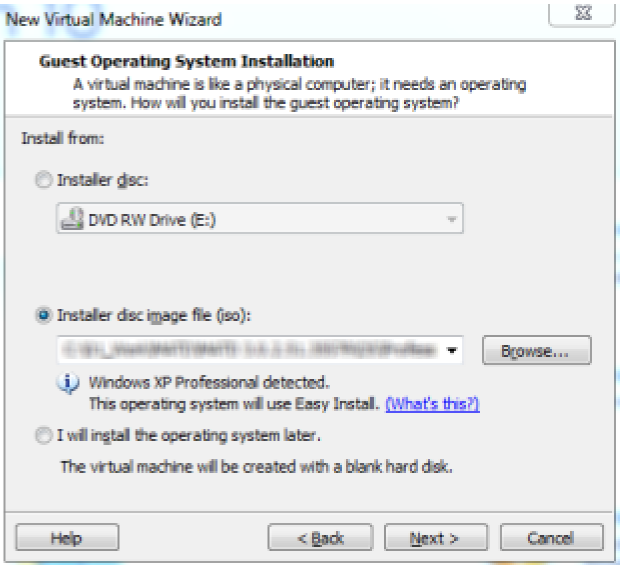
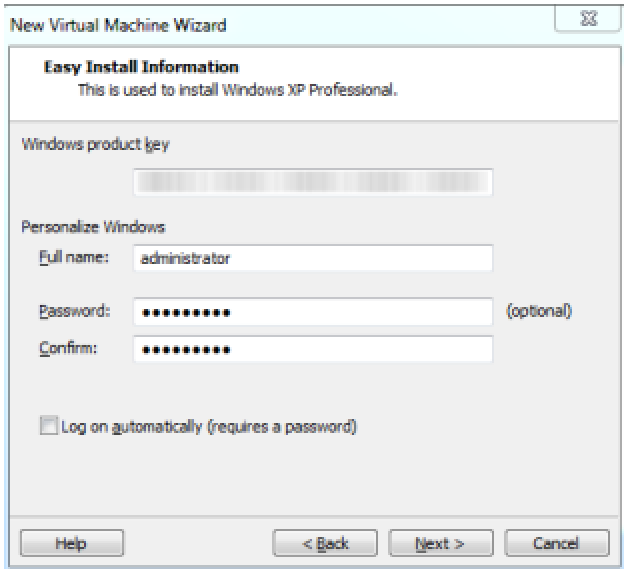
Step	Details
Step 5: In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next.**	 New Virtual Machine Wizard **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: ○ Installer disc: DVD RW Drive (E:) ● Installer disc image file (iso): Windows XP Professional detected. This operating system will use Easy Install. (What's this?) ○ I will install the operating system later. The virtual machine will be created with a blank hard disk.
Step 6: Enter the information in the **Easy Install Information** window and then click **Next.**	• **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file. • **Full name** — You must enter `administrator` as the **Full name.** • **Password** — You must enter `cr@cker42` as the password. This is the password that Advanced Threat Defense uses to log on to the VM. • **Confirm** — Enter `cr@cker42` again to confirm. • **Log on automatically (requires a password)** — Deselect this box.  New Virtual Machine Wizard **Easy Install Information** This is used to install Windows XP Professional. Windows product key Personalize Windows Full name: administrator Password: ••••••••• (optional) Confirm: ••••••••• □ Log on automatically (requires a password)

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

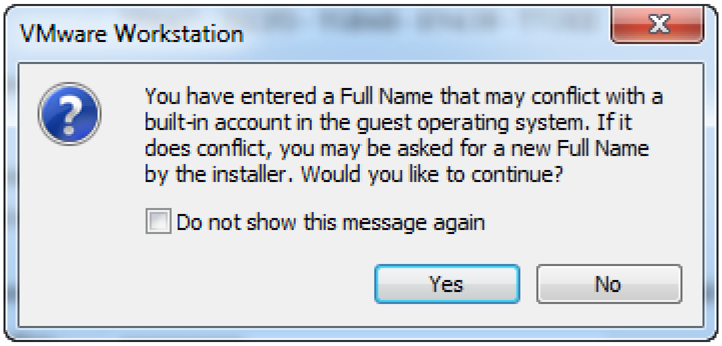
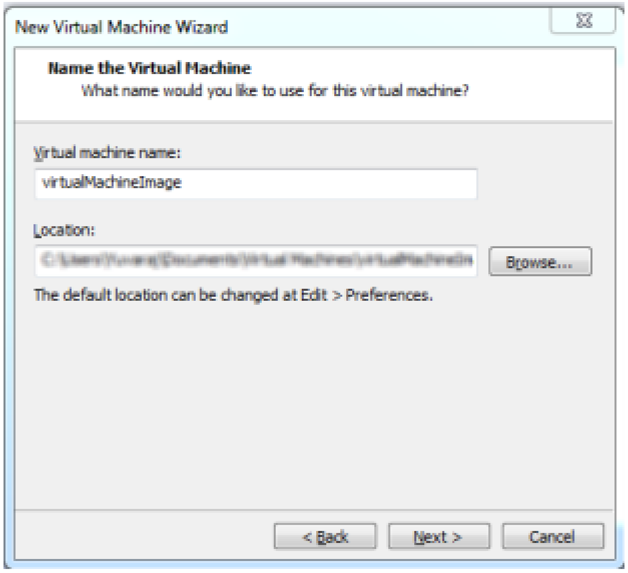
Step	Details
Step 7: If the **VMware Workstation** message displays, click **Yes**.	 VMware Workstation You have entered a Full Name that may conflict with a built-in account in the guest operating system. If it does conflict, you may be asked for a new Full Name by the installer. Would you like to continue? □ Do not show this message again
Step 8: Enter the information in the **Name the Virtual Machine** window and then click **Next**.	• **Virtual Machine name** — You must enter `virtualMachineImage` as the name. • **Location** — Browse and select the folder where you want to create the VMDK file.  New Virtual Machine Wizard **Name the Virtual Machine** What name would you like to use for this virtual machine? Virtual machine name: virtualMachineImage Location: The default location can be changed at Edit > Preferences.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

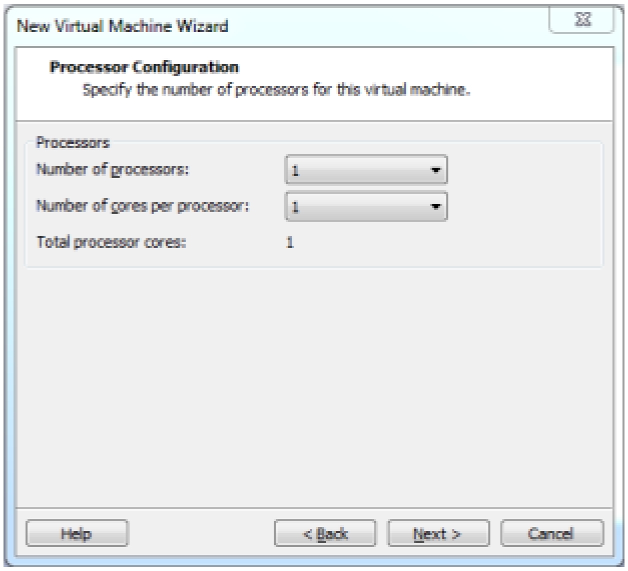
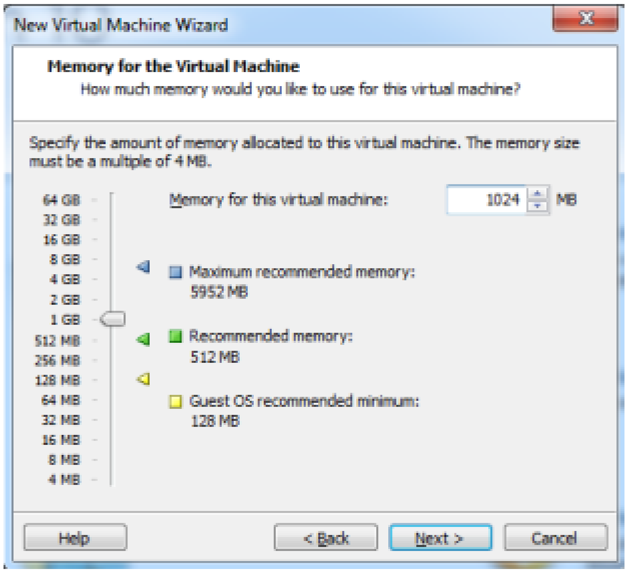
Step	Details
Step 9: In the **Processor Configuration** window, leave the default values and click **Next**.	 New Virtual Machine Wizard **Processor Configuration** Specify the number of processors for this virtual machine. Processors Number of processors: 1 Number of cores per processor: 1 Total processor cores: 1
Step 10: In the **Memory for the Virtual Machine** window, set 1024 MB as the memory.	 New Virtual Machine Wizard **Memory for the Virtual Machine** How much memory would you like to use for this virtual machine? Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB. Memory for this virtual machine: 1024 MB Maximum recommended memory: 5952 MB Recommended memory: 512 MB Guest OS recommended minimum: 128 MB 64 GB 32 GB 16 GB 8 GB 4 GB 2 GB 1 GB 512 MB 256 MB 128 MB 64 MB 32 MB 16 MB 8 MB 4 MB Help < Back Next > Cancel

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

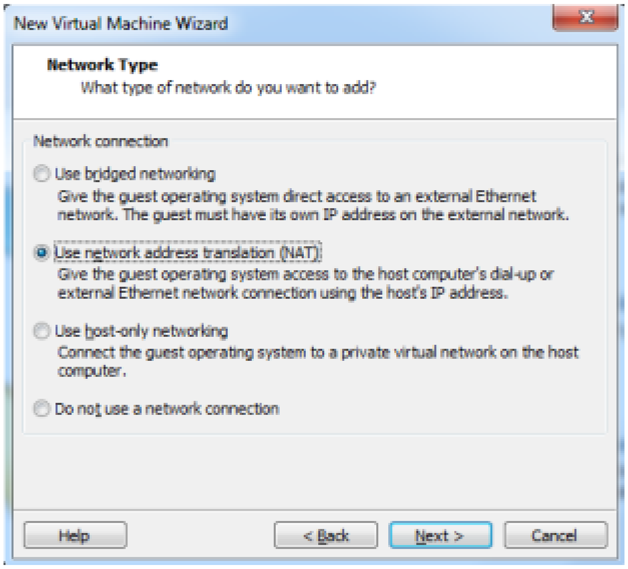
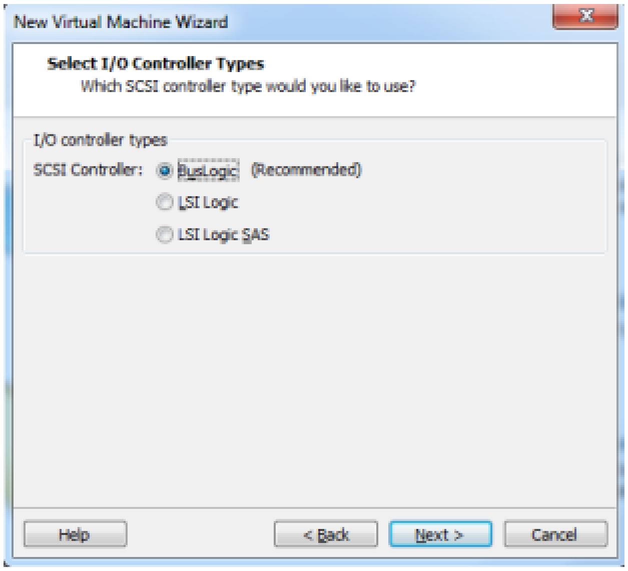
Step	Details
Step 11: In the **Network Type** window, leave the default selection.	 New Virtual Machine Wizard **Network Type** What type of network do you want to add? Network connection ○ Use bridged networking Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network. ● Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address. ○ Use host-only networking Connect the guest operating system to a private virtual network on the host computer. ○ Do not use a network connection
Step 12: In the **Select I/O Controller Types** , leave the default selection.	 New Virtual Machine Wizard **Select I/O Controller Types** Which SCSI controller type would you like to use? I/O controller types SCSI Controller: ● BusLogic (Recommended) ○ LSI Logic ○ LSI Logic SAS

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

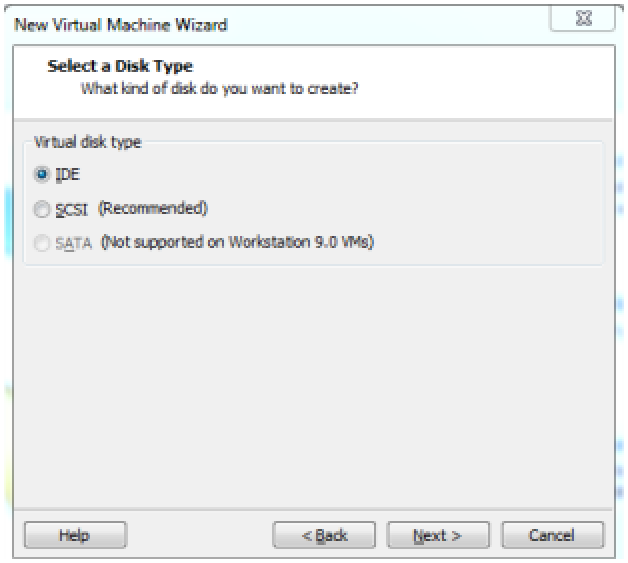
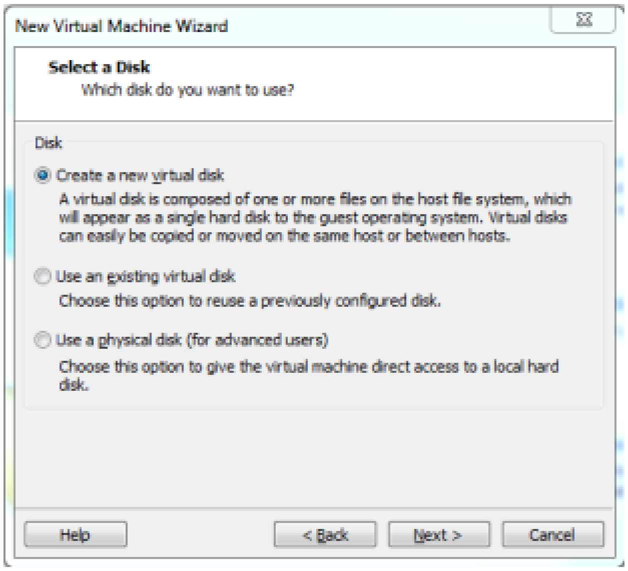
Step	Details
Step 13: In the **Select a Disk Type** page, select **IDE** and click **Next.** SCSI disks are not compatible with Advanced Threat Defense.	 **Select a Disk Type** What kind of disk do you want to create? Virtual disk type ● IDE ○ SCSI (Recommended) ○ SATA (Not supported on Workstation 9.0 VMs)
Step 14: In the **Select a Disk** window, select **Create a new virtual disk** and click **Next.**	 **Select a Disk** Which disk do you want to use? Disk ● Create a new virtual disk A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts. ○ Use an existing virtual disk Choose this option to reuse a previously configured disk. ○ Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard disk.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

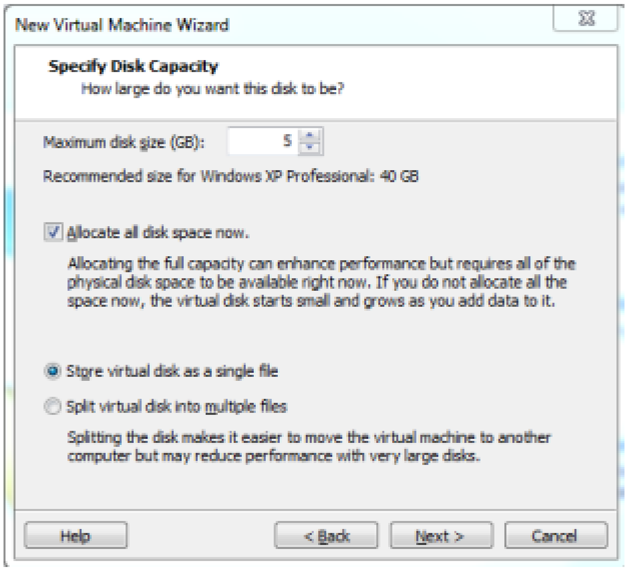
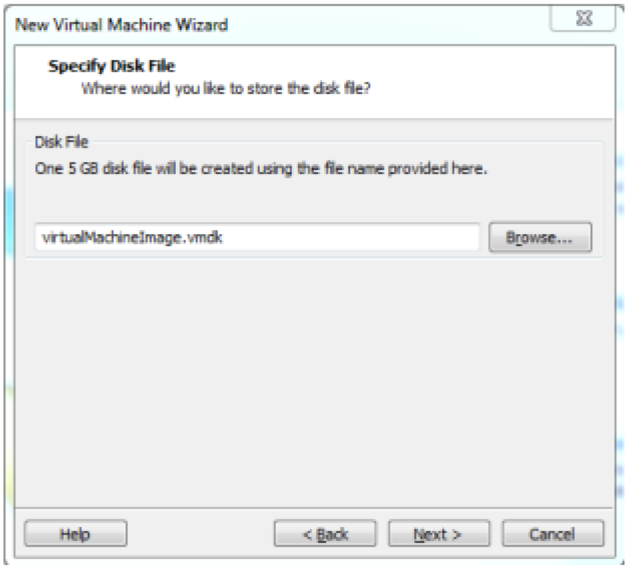
Step	Details
Step 15: Specify the details in the **Specify Disk Capacity** window and then click **Next**.	- **Maximum disk size (GB)** — For Windows XP, the maximum disk size can be 30 GB, however you must enter 5 GB for optimal performance. - Select **Allocate all disk space now**. - Select **Store virtual disk as a single file**.  New Virtual Machine Wizard **Specify Disk Capacity** How large do you want this disk to be? Maximum disk size (GB): 5 Recommended size for Windows XP Professional: 40 GB ☑ Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it. ● Store virtual disk as a single file ○ Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Step 16: In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**. If you specified a different name for **Virtual Machine name**, that name is displayed here.	 New Virtual Machine Wizard **Specify Disk File** Where would you like to store the disk file? Disk File One 5 GB disk file will be created using the file name provided here. virtualMachineImage.vmdk

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

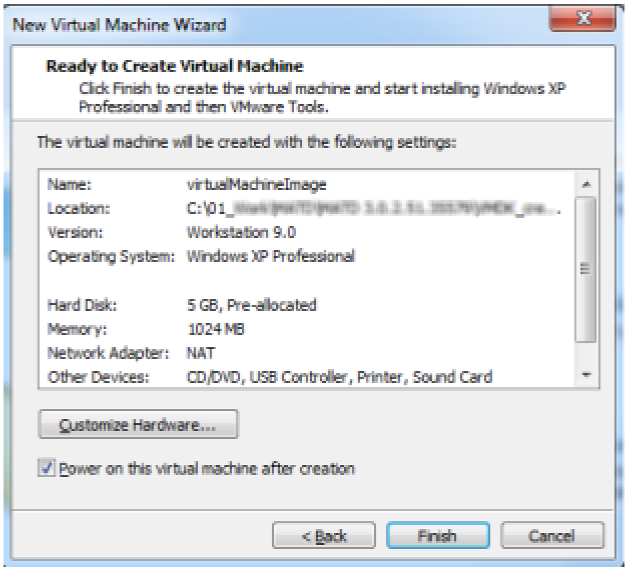
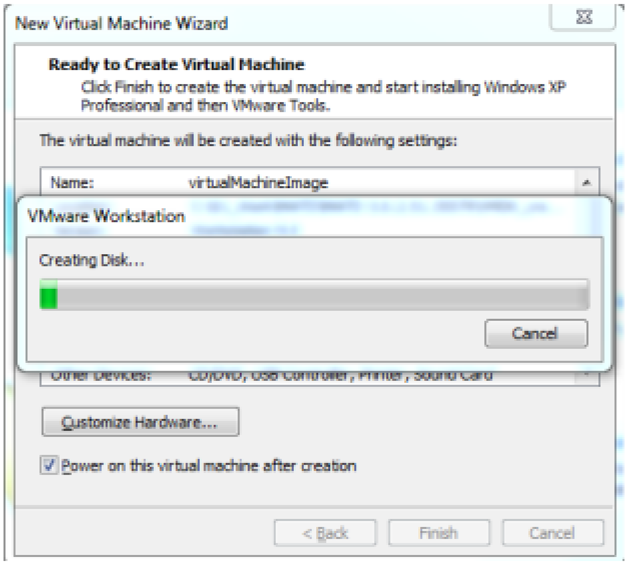
Step	Details
Step 17: Complete the following in the **Ready to Create Virtual Machine** window.	• **Power on this virtual machine after creation** — Select this option. • Click **Finish.** This step might take around 30 minutes to complete.  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows XP Professional and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage Location: C:\01_[redacted] Version: Workstation 9.0 Operating System: Windows XP Professional Hard Disk: 5 GB, Pre-allocated Memory: 1024 MB Network Adapter: NAT Other Devices: CD/DVD, USB Controller, Printer, Sound Card Customize Hardware... ☑ Power on this virtual machine after creation < Back Finish Cancel  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows XP Professional and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage VMware Workstation Creating Disk... Cancel Other Devices: CD/DVD, USB Controller, Printer, Sound Card Customize Hardware... ☑ Power on this virtual machine after creation < Back Finish Cancel
Step 18: If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**.	Windows begins to install, which might take around 15 minutes.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

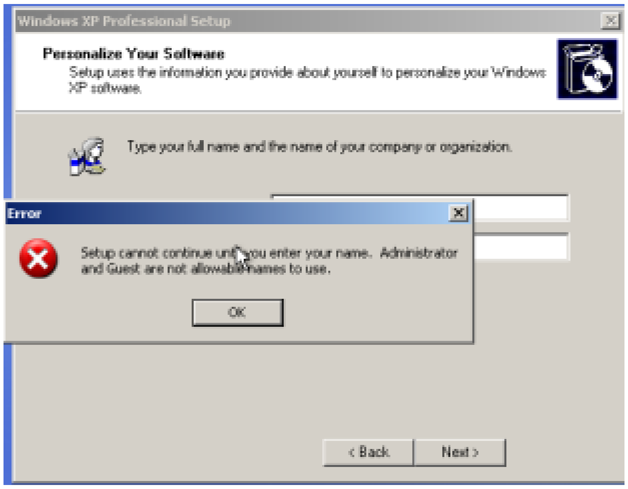
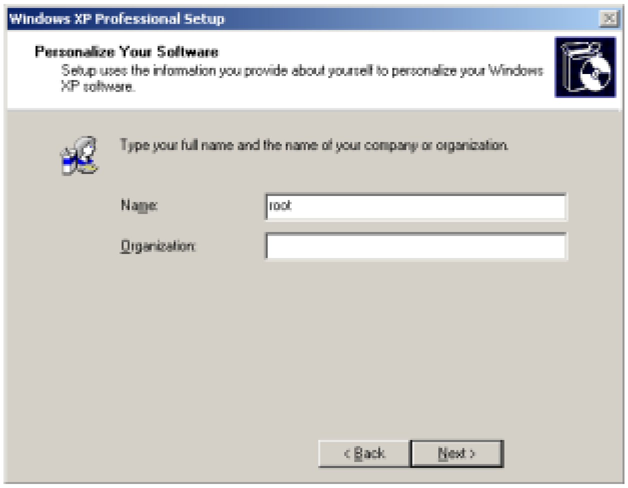
Step	Details
Step 19: Click **OK** if the following error message is displayed — *Setup cannot continue until you enter your name. Administrator and Guest are not allowable names to use.*	 Windows XP Professional Setup Personalize Your Software Setup uses the information you provide about yourself to personalize your Windows XP software. Type your full name and the name of your company or organization. Error Setup cannot continue until you enter your name. Administrator and Guest are not allowable names to use.
Step 20: Enter the following details in the **Windows XP Professional Setup** page.	• **Name:** Enter `root` • **Organization:** Leave this blank and click **Next**. This operation might take around 15 minutes.  Windows XP Professional Setup Personalize Your Software Setup uses the information you provide about yourself to personalize your Windows XP software. Type your full name and the name of your company or organization. Name: root Organization:
Step 21: Only if prompted, log on to virtualMachineImage with the following credentials.	• **User:** `administrator` • **Password:** `cr@cker42`

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

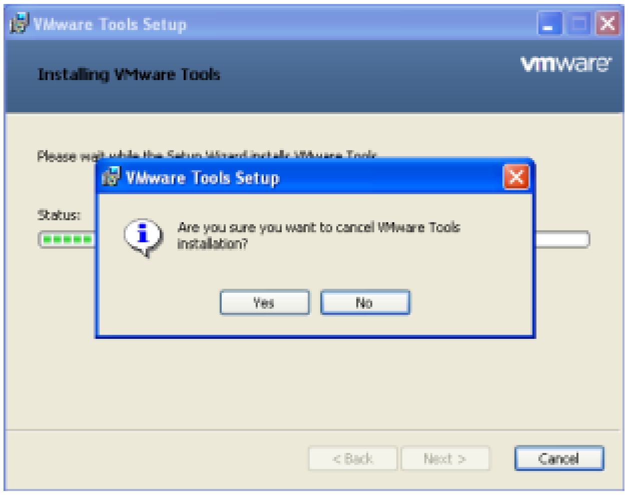
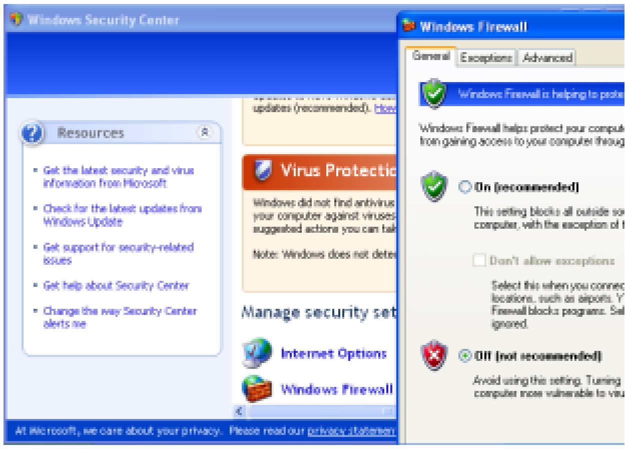
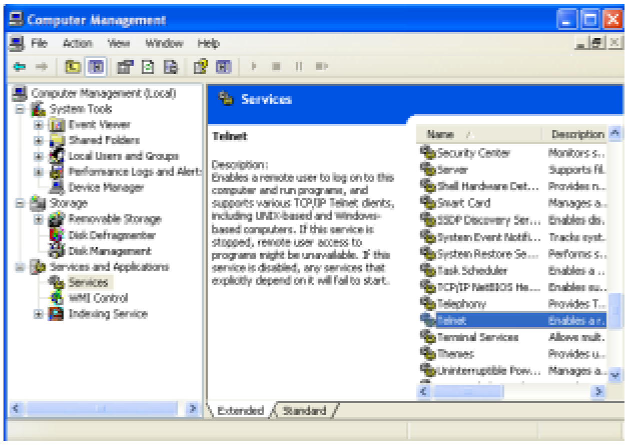
Step	Details
Step 22: Stop the VMware Tools installation. The VMware Tools are not compatible with Advanced Threat Defense. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready.	 VMware Tools Setup Installing VMware Tools Please wait while the Setup Wizard installs VMware Tools Status: VMware Tools Setup Are you sure you want to cancel VMware Tools installation?
Step 23: In the virtualMachineImage, select **Start | Control Panel | Security Center | Windows Firewall | OFF.**	 Windows Security Center Windows Firewall General Exceptions Advanced Resources Get the latest security and virus information from Microsoft Check for the latest updates from Windows Update Get support for security-related issues Get help about Security Center Change the way Security Center alerts me Virus Protectio Manage security set Internet Options Windows Firewall updates (recommended). How Windows did not find antivirus your computer against viruses suggested actions you can tak Note: Windows does not dete Windows Firewall is helping to prote Windows Firewall helps protect your comput from gaining access to your computer throug ○ On (recommended) This setting blocks all outside so computer, with the exception of t □ Don't allow exceptions Select this when you connec locations, such as airports. Y Firewall blocks programs. Sel ignored. ● Off (not recommended) Avoid using this setting. Turning computer more vulnerable to viru At Microsoft, we care about your privacy. Please read our privacy statemen
Step 24: In the virtualMachineImage VM, click **Start** and right-click **My Computer**. Then select **Manage | Services and Applications | Services**. Then double-click **Telnet**.	 Computer Management File Action View Window Help Computer Management (Local) System Tools Event Viewer Shared Folders Local Users and Groups Performance Logs and Alert: Device Manager Storage Removable Storage Disk Defragmenter Disk Management Services and Applications Services WMI Control Indexing Service Extended Standard Services Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. Name / Description Security Center Monitors s... Server Supports fil... Shell Hardware Det... Provides n... Smart Card Manages a... SSDP Discovery Ser... Enables dis... System Event Notifi... Tracks syst... System Restore Se... Performs s... Task Scheduler Enables a ... TCP/IP NetBIOS He... Enables su... Telephony Provides T... Telnet Enables a r... Terminal Services Allows mult... Themes Provides u... Uninterruptible Pow... Manages a...

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

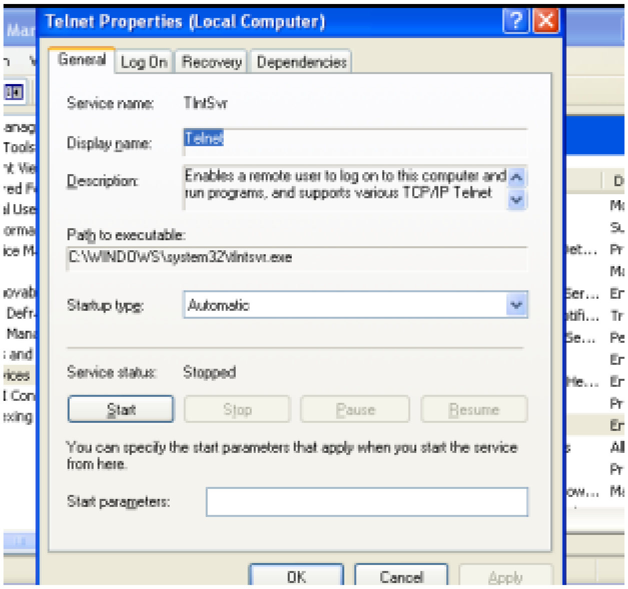
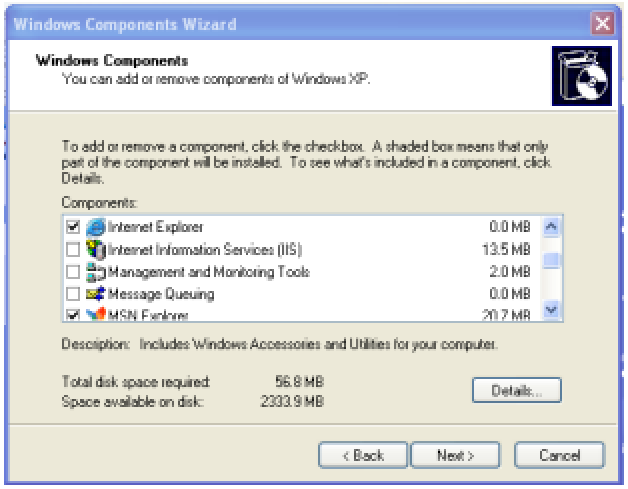
Step	Details
Step 25: In the **Telnet Properties(Local Computer)** window, you must select **Automatic** from the **Startup type** drop-down list. Then select **Apply** | **Start** | **OK**.	 Telnet Properties (Local Computer) General Log On Recovery Dependencies Start Stop Pause Resume OK Cancel Apply Service name: TlntSvr Display name: Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet Path to executable: C:\WINDOWS\system32\tlntsvr.exe Startup type: Automatic Service status: Stopped You can specify the start parameters that apply when you start the service from here. Start parameters:
Step 26: Enable FTP on the VM. In the virtualMachineImage, select **Start** | **Control Panel** | **Add or remove Programs** | **Add or remove Windows components.**.	 Windows Components Wizard Details... < Back Next > Cancel **Windows Components** You can add or remove components of Windows XP. To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components: ☑ Internet Explorer 0.0 MB ☐ Internet Information Services (IIS) 13.5 MB ☐ Management and Monitoring Tools 2.0 MB ☐ Message Queuing 0.0 MB ☑ MSN Explorer 20.7 MB Description: Includes Windows Accessories and Utilities for your computer. Total disk space required: 56.8 MB Space available on disk: 2333.9 MB

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

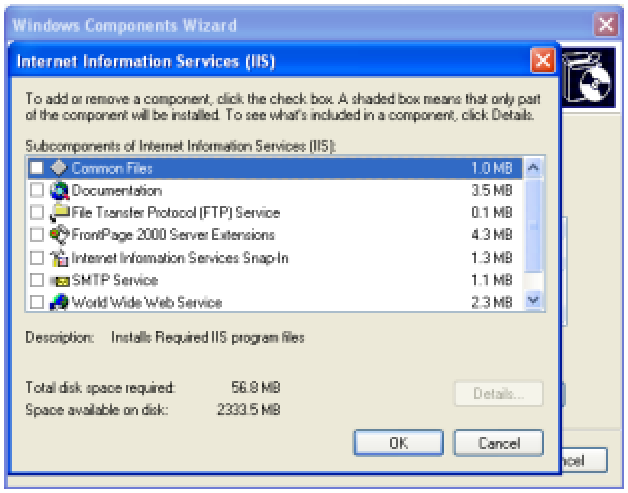
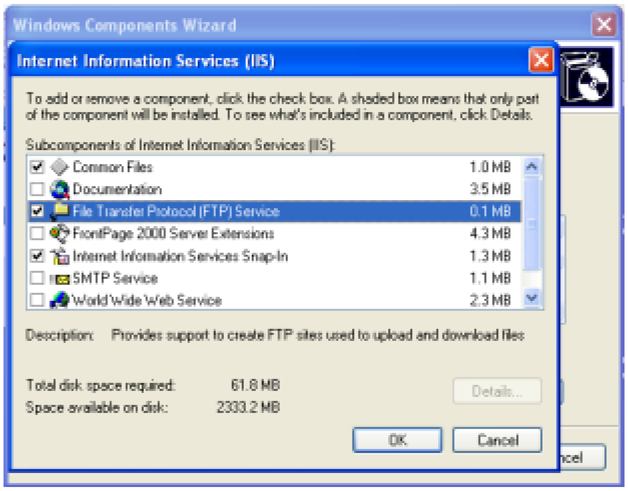
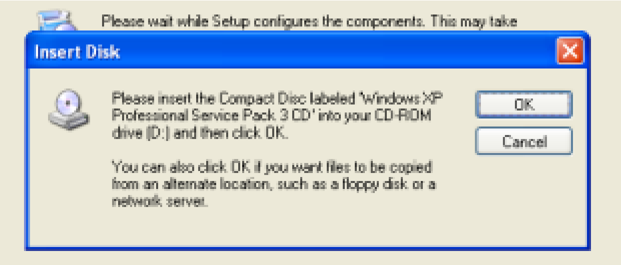
Step	Details
Step 27: In the **Windows Components** wizard, double-click **Internet Information Services(IIS)**.	 Windows Components Wizard Internet Information Services (IIS) To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Internet Information Services (IIS): □ Common Files 1.0 MB □ Documentation 3.5 MB □ File Transfer Protocol (FTP) Service 0.1 MB □ FrontPage 2000 Server Extensions 4.3 MB □ Internet Information Services Snap-In 1.3 MB □ SMTP Service 1.1 MB □ World Wide Web Service 2.3 MB Description: Installs Required IIS program files Total disk space required: 56.8 MB Space available on disk: 2333.5 MB
Step 28: In the **Internet Information Services(IIS)** pop-up window, complete the following.	1 Select **File Transfer Protocol (FTP) Service**. 2 Select **Common Files**. 3 Select **Internet Information Services Snap-In**, click **OK**, and then click **Next**.  Windows Components Wizard Internet Information Services (IIS) To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Internet Information Services (IIS): ☑ Common Files 1.0 MB □ Documentation 3.5 MB ☑ File Transfer Protocol (FTP) Service 0.1 MB □ FrontPage 2000 Server Extensions 4.3 MB ☑ Internet Information Services Snap-In 1.3 MB □ SMTP Service 1.1 MB □ World Wide Web Service 2.3 MB Description: Provides support to create FTP sites used to upload and download files Total disk space required: 61.8 MB Space available on disk: 2333.2 MB
Step 29: In the **Insert Disk** pop-up, click **Cancel**.	 Please wait while Setup configures the components. This may take Insert Disk Please insert the Compact Disc labeled 'Windows XP Professional Service Pack 3 CD' into your CD-ROM drive (D:) and then click OK. You can also click OK if you want files to be copied from an alternate location, such as a floppy disk or a network server.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

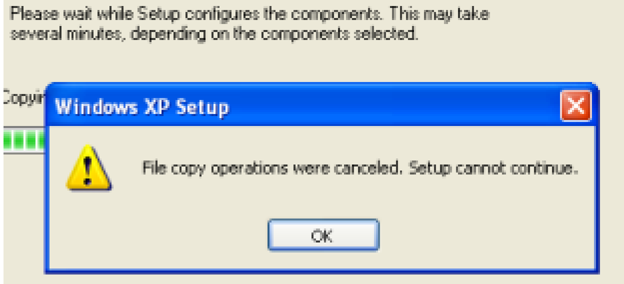
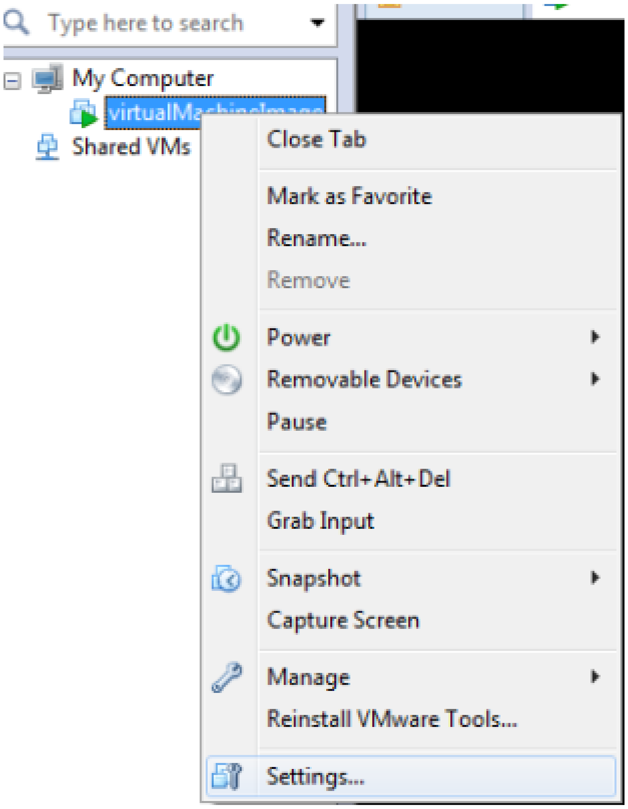
Step	Details
Step 30: In the **Windows XP Setup** pop-up, select **OK**.	 Please wait while Setup configures the components. This may take several minutes, depending on the components selected. Copyi Windows XP Setup File copy operations were canceled. Setup cannot continue.
Step 31: In the VMware Workstation, right-click on the VM, which in this example is virtualMachineImage. Then select **Settings**.	 Type here to search My Computer virtualMachineImage Shared VMs Close Tab Mark as Favorite Rename... Remove Power Removable Devices Pause Send Ctrl+Alt+Del Grab Input Snapshot Capture Screen Manage Reinstall VMware Tools... Settings...

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

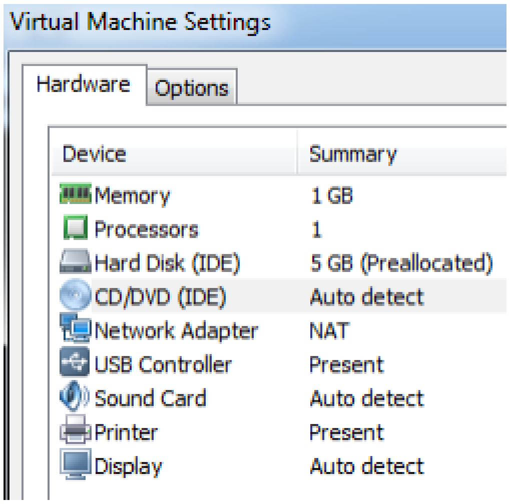
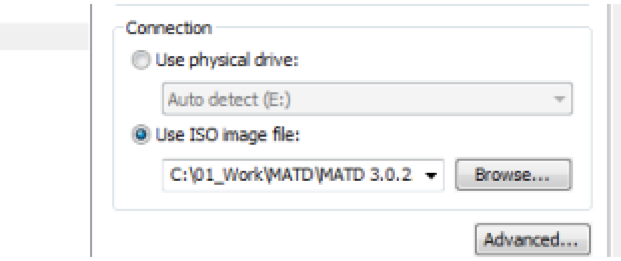
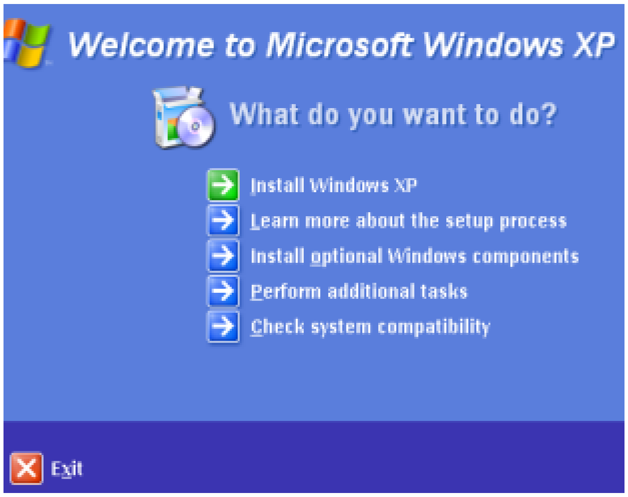
Step	Details
Step 32: In the Virtual Machine Settings window, select **CD/DVD (IDE)**.	 Virtual Machine Settings Hardware | Options Device — Summary Memory — 1 GB Processors — 1 Hard Disk (IDE) — 5 GB (Preallocated) CD/DVD (IDE) — Auto detect Network Adapter — NAT USB Controller — Present Sound Card — Auto detect Printer — Present Display — Auto detect
Step 33: In the **Use ISO image file** field, browse to the ISO file that you used and press **OK**.	 Connection ○ Use physical drive: Auto detect (E:) ● Use ISO image file: C:\01_Work\MATD\MATD 3.0.2 Browse... Advanced...
Step 34: In the **Welcome to Microsoft Windows XP** page, click **Exit**.	 Welcome to Microsoft Windows XP What do you want to do? Install Windows XP Learn more about the setup process Install optional Windows components Perform additional tasks Check system compatibility Exit

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

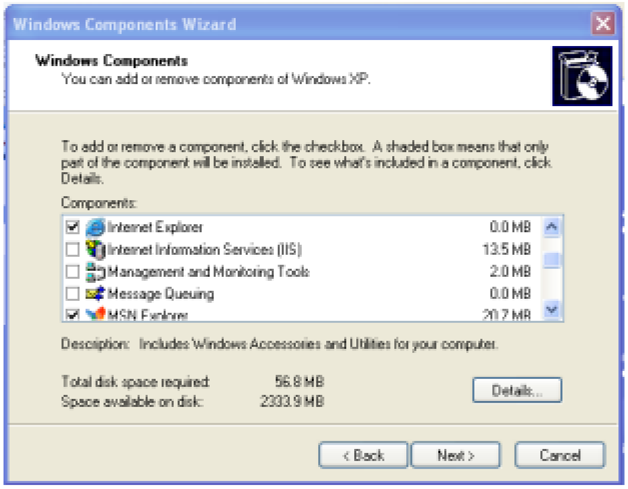
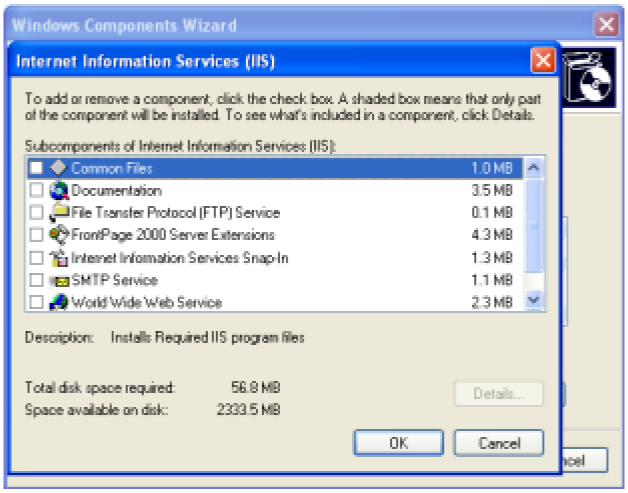
Step	Details
Step 35: In the virtualMachineImage, select **Start | Control Panel | Add or remove Programs | Add or remove Windows components.**.	 Windows Components Wizard Details... < Back Next > Cancel **Windows Components** You can add or remove components of Windows XP. To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components: ☑ Internet Explorer 0.0 MB ☐ Internet Information Services (IIS) 13.5 MB ☐ Management and Monitoring Tools 2.0 MB ☐ Message Queuing 0.0 MB ☑ MSN Explorer 20.7 MB Description: Includes Windows Accessories and Utilities for your computer. Total disk space required: 56.8 MB Space available on disk: 2333.9 MB
Step 36: In the **Windows Components** wizard, double-click **Internet Information Services(IIS).**	 Windows Components Wizard Internet Information Services (IIS) Details... OK Cancel To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Internet Information Services (IIS): ☐ Common Files 1.0 MB ☐ Documentation 3.5 MB ☐ File Transfer Protocol (FTP) Service 0.1 MB ☐ FrontPage 2000 Server Extensions 4.3 MB ☐ Internet Information Services Snap-In 1.3 MB ☐ SMTP Service 1.1 MB ☐ World Wide Web Service 2.3 MB Description: Installs Required IIS program files Total disk space required: 56.8 MB Space available on disk: 2333.5 MB

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

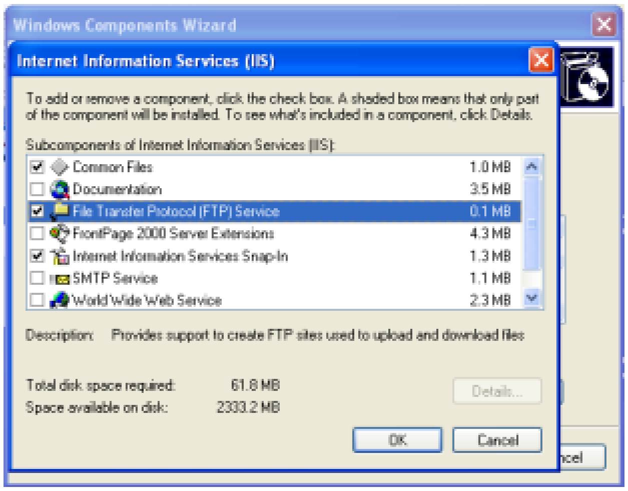
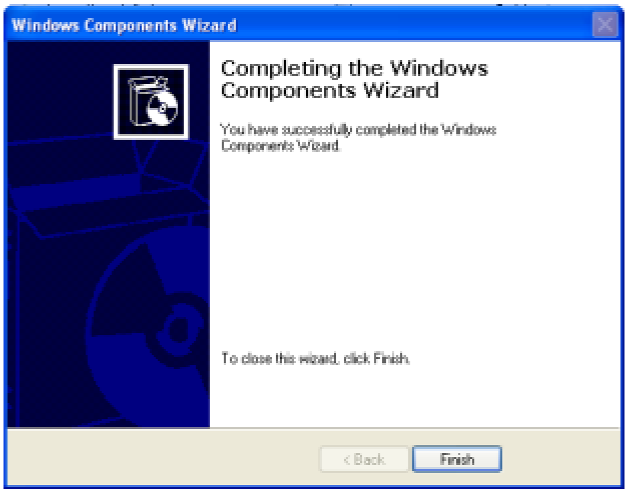
Step	Details
Step 37: In the **Internet Information Services(IIS)** pop-up window, complete the following.	1 Select **File Transfer Protocol (FTP) Service**. 2 Select **Common Files**. 3 Select **Internet Information Services Snap-In**, click **OK**, and then click **Next**.  Windows Components Wizard Internet Information Services (IIS) To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Internet Information Services (IIS): ☑ Common Files 1.0 MB ☐ Documentation 3.5 MB ☑ File Transfer Protocol (FTP) Service 0.1 MB ☐ FrontPage 2000 Server Extensions 4.3 MB ☑ Internet Information Services Snap-In 1.3 MB ☐ SMTP Service 1.1 MB ☐ World Wide Web Service 2.3 MB Description: Provides support to create FTP sites used to upload and download files Total disk space required: 61.8 MB Space available on disk: 2333.2 MB
Step 38: In the **Windows Components Wizard**, click **Finish** to finish installing FTP.	 Windows Components Wizard Completing the Windows Components Wizard You have successfully completed the Windows Components Wizard. To close this wizard, click Finish.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

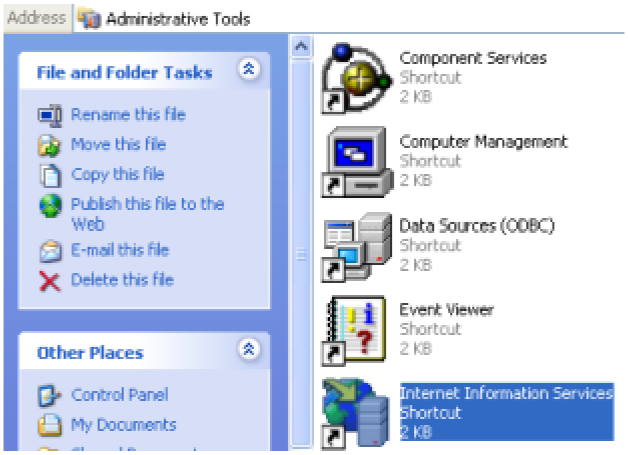
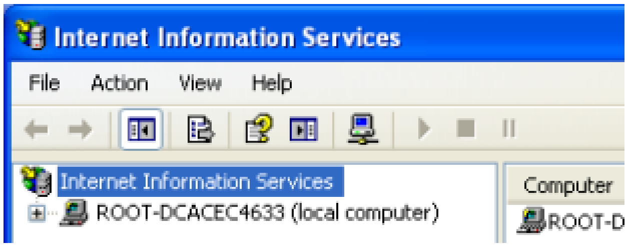
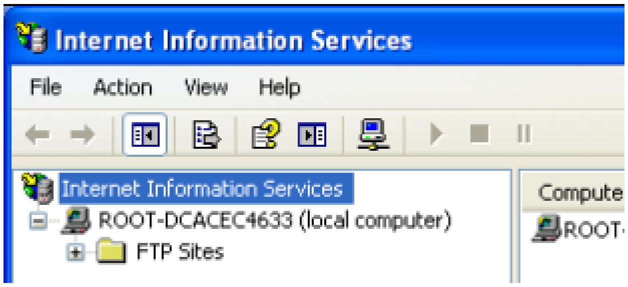
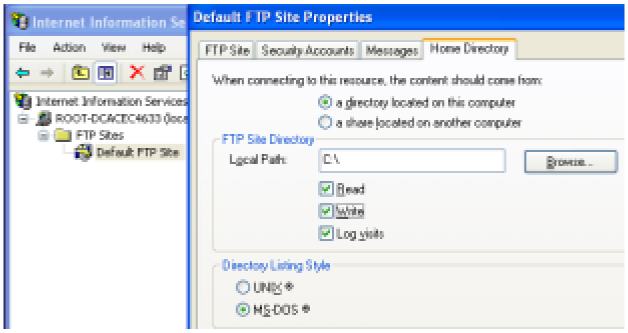
Step	Details
Step 39: Select **Start** | **Control Panel** | **Switch to Classic View** | **Administrative Tools** and double-click **Internet Information Services.**	 Address Administrative Tools File and Folder Tasks Rename this file Move this file Copy this file Publish this file to the Web E-mail this file Delete this file Other Places Control Panel My Documents Component Services Shortcut 2 KB Computer Management Shortcut 2 KB Data Sources (ODBC) Shortcut 2 KB Event Viewer Shortcut 2 KB Internet Information Services Shortcut 2 KB
Step 40: In the **Internet Information Services** widnow, expand + below **Internet Information Services.**	 Internet Information Services File Action View Help Internet Information Services ROOT-DCACEC4633 (local computer) Computer ROOT-D
Step 41: Expand **FTP Sites.**	 Internet Information Services File Action View Help Internet Information Services ROOT-DCACEC4633 (local computer) FTP Sites Compute ROOT
Step 42: Right-click on **Default FTP Site** and then select **Properties** | **Home Directory** . Then complete the following. 1 Browse to C:\\ 2 Select **Read**. 3 Select **Write**. 4 Select **Log visits** and click **Apply** and then **OK.**	 Internet Information Se File Action View Help Internet Information Services ROOT-DCACEC4633 (loca FTP Sites Default FTP Site Default FTP Site Properties FTP Site Security Accounts Messages Home Directory Browse... When connecting to this resource, the content should come from: ● a directory located on this computer ○ a share located on another computer FTP Site Directory Local Path: C:\\ ☑ Read ☑ Write ☑ Log visits Directory Listing Style ○ UNIX ® ● MS-DOS ®

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

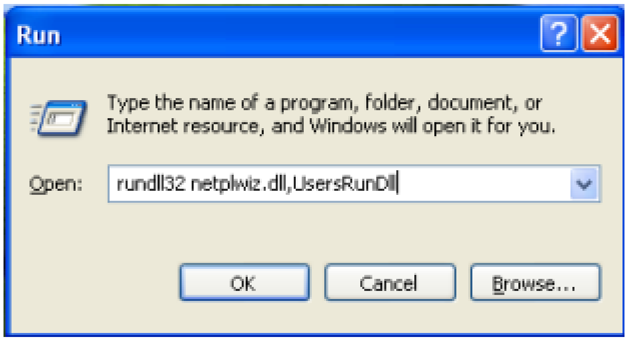
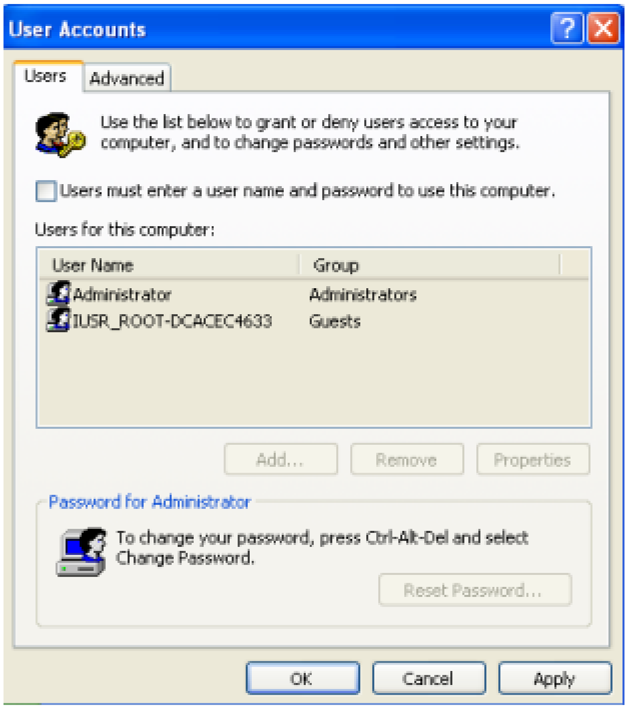
Step	Details
Step 43: Set automatic logon by selecting **Start** | **Run**, enter `rundll32 netplwiz.dll,UsersRunDll` and press **Enter**.	 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: rundll32 netplwiz.dll,UsersRunDll
Step 44: In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**.	 Use the list below to grant or deny users access to your computer, and to change passwords and other settings. □ Users must enter a user name and password to use this computer. Users for this computer: User Name — Group Administrator — Administrators IUSR_ROOT-DCACEC4633 — Guests Password for Administrator To change your password, press Ctrl-Alt-Del and select Change Password. User Accounts Users Advanced Add... Remove Properties Reset Password... OK Cancel Apply

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

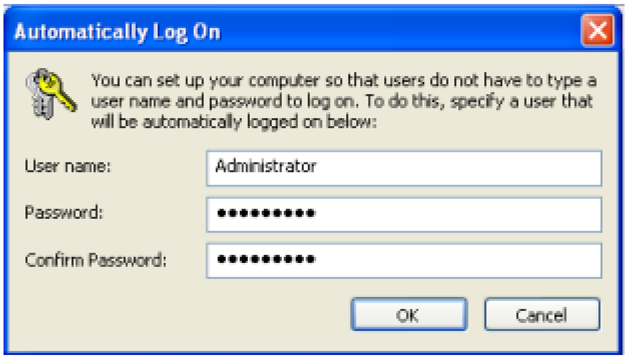
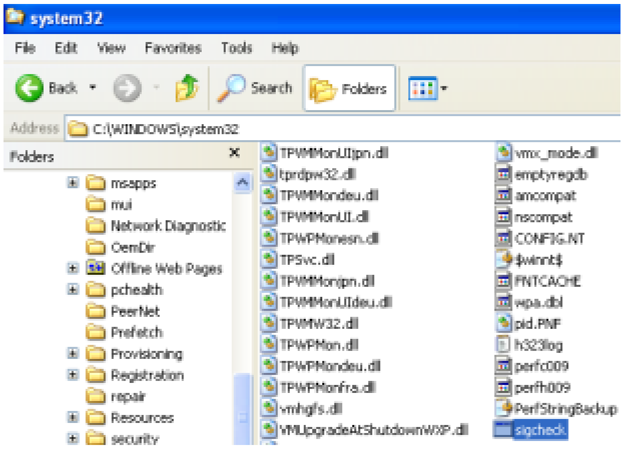
Step	Details
Step 45: In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes.	- **User name** — Enter `Administrator` - **Password** — Enter `cr@cker42` - **Confirm Password** — Enter `cr@cker42`  Automatically Log On You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below: User name: Administrator Password: •••••••••• Confirm Password: ••••••••••
Step 46: Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx.	The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation.
Step 47: Extract sigcheck.zip to `C:\WINDOWS\system32` location.	 Address C:\WINDOWS\system32 system32 File Edit View Favorites Tools Help Back Search Folders Folders msapps mui Network Diagnostic OemDir Offline Web Pages pchealth PeerNet Prefetch Provisioning Registration repair Resources security TPVMMonUIjpn.dll tprdpw32.dll TPVMMondeu.dll TPVMMonUI.dll TPWPMonesn.dll TPSvc.dll TPVMMonjpn.dll TPVMMonUIdeu.dll TPVMW32.dll TPWPMon.dll TPWPMondeu.dll TPWPMonfra.dll vmhgfs.dll VMUpgradeAtShutdownWXP.dll vmx_mode.dll emptyregdb amcompat nscompat CONFIG.NT $winnt$ FNTCACHE wpa.dbl pid.PNF h323log perfc009 perfh009 PerfStringBackup sigcheck
Step 48: In Windows Explorer, go to C:\ WINDOWS\system32 and double-click **sigcheck.exe**.	
Step 49: If prompted, click **Run** in the warning message.	

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

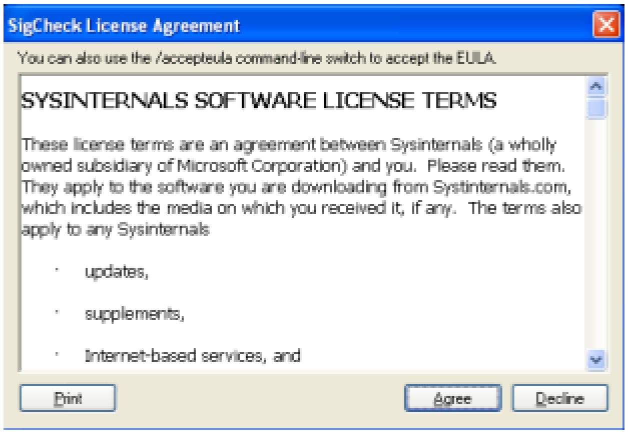
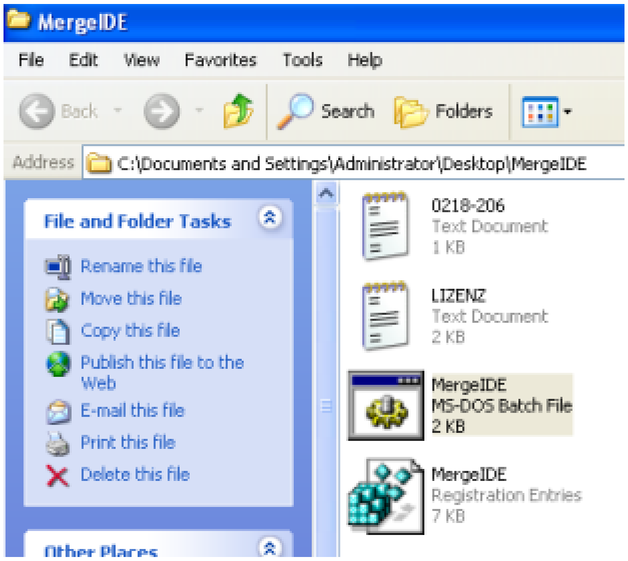
Step	Details
Step 50: Click **Agree** for **Sigcheck License Agreement**. After you click on **Agree**, no confirmation message is displayed.	 SigCheck License Agreement You can also use the /accepteula command-line switch to accept the EULA. SYSINTERNALS SOFTWARE LICENSE TERMS These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals · updates, · supplements, · Internet-based services, and
Step 51: Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM.	 MergeIDE File Edit View Favorites Tools Help Back Search Folders Address C:\Documents and Settings\Administrator\Desktop\MergeIDE File and Folder Tasks Rename this file Move this file Copy this file Publish this file to the Web E-mail this file Print this file Delete this file Other Places 0218-206 Text Document 1 KB LIZENZ Text Document 2 KB MergeIDE MS-DOS Batch File 2 KB MergeIDE Registration Entries 7 KB
Step 52: Extract MergeIDE.zip and run the MergeIDE batch file in the VM.	• If prompted, select **Run** in the warning message. • Close Windows Explorer.
Step 53: Disable Windows updates.	1 Select **Start** | **Settings** | **Control Panel**. 2 Open **System**. 3 In the **Automatic Updates** tab, deselect **Keep my computer up to date.** 4 Click **Apply** and then **OK**.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

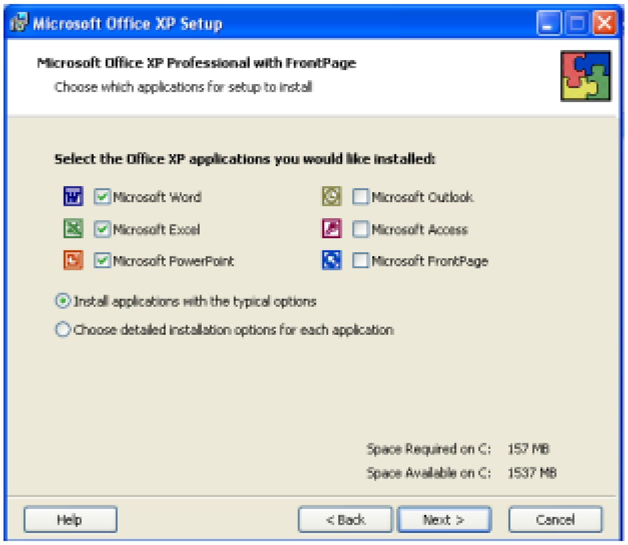
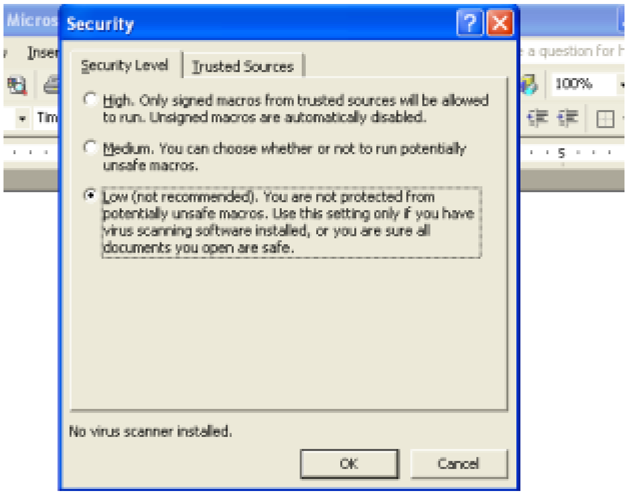
Step	Details
Step 54: To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine.	 Microsoft Office XP Setup Microsoft Office XP Professional with FrontPage Choose which applications for setup to install Select the Office XP applications you would like installed: ☑ Microsoft Word ☐ Microsoft Outlook ☑ Microsoft Excel ☐ Microsoft Access ☑ Microsoft PowerPoint ☐ Microsoft FrontPage ● Install applications with the typical options ○ Choose detailed installation options for each application Space Required on C: 157 MB Space Available on C: 1537 MB
Step 55: Lower the security to run macros for the Office applications.	• Open Microsoft Word 2003 and select **Tools** | **Macro** | **Security** and then select **Low** and click **OK**.  Security Security Level | Trusted Sources ○ High. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled. ○ Medium. You can choose whether or not to run potentially unsafe macros. ● Low (not recommended). You are not protected from potentially unsafe macros. Use this setting only if you have virus scanning software installed, or you are sure all documents you open are safe. No virus scanner installed. • Similarly lower the macro security for Microsoft Excel and Powerpoint.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

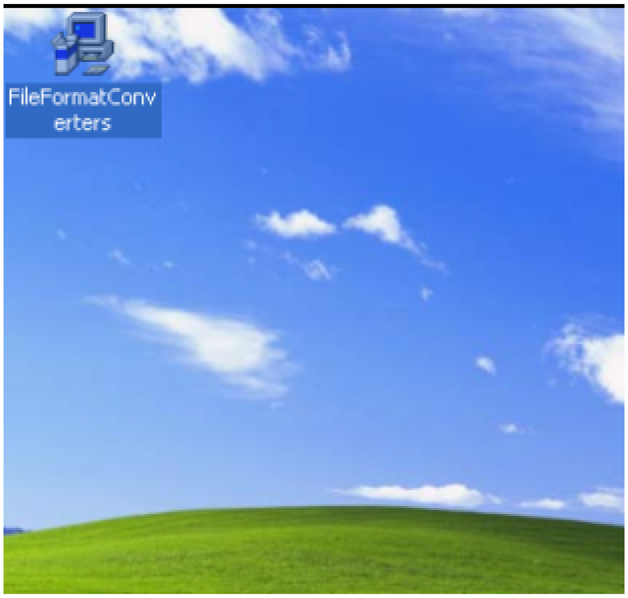
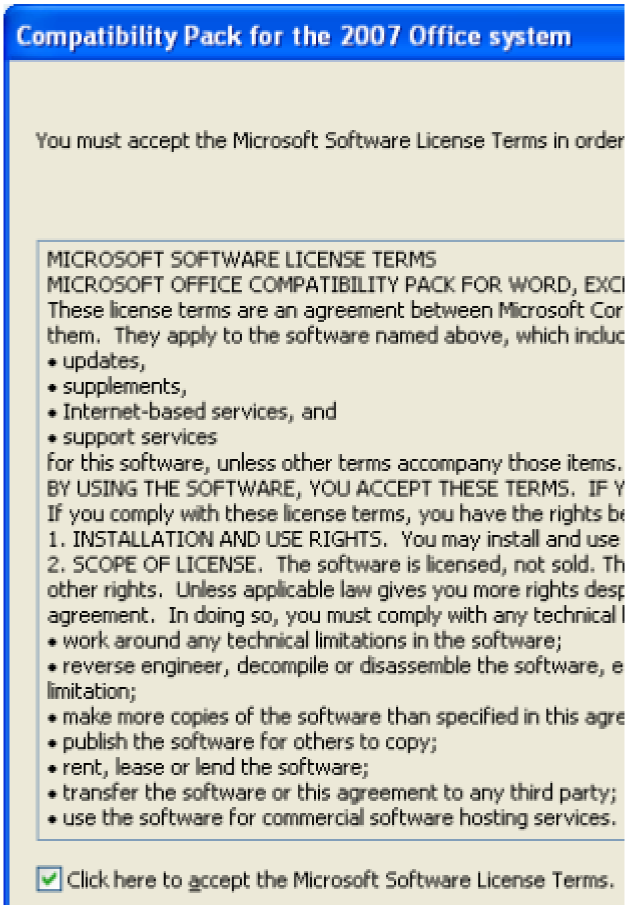
Step	Details
Step 56: You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed. Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine.	
Step 57: In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **OK**.	Compatibility Pack for the 2007 Office system You must accept the Microsoft Software License Terms in order MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT OFFICE COMPATIBILITY PACK FOR WORD, EXCI These license terms are an agreement between Microsoft Cor them. They apply to the software named above, which incluc • updates, • supplements, • Internet-based services, and • support services for this software, unless other terms accompany those items. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF Y If you comply with these license terms, you have the rights be 1. INSTALLATION AND USE RIGHTS. You may install and use 2. SCOPE OF LICENSE. The software is licensed, not sold. Th other rights. Unless applicable law gives you more rights desp agreement. In doing so, you must comply with any technical l • work around any technical limitations in the software; • reverse engineer, decompile or disassemble the software, e limitation; • make more copies of the software than specified in this agre • publish the software for others to copy; • rent, lease or lend the software; • transfer the software or this agreement to any third party; • use the software for commercial software hosting services. ☑ Click here to accept the Microsoft Software License Terms.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

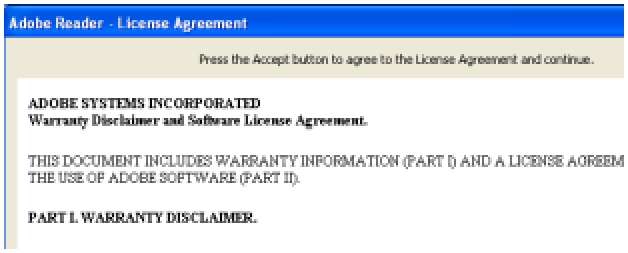
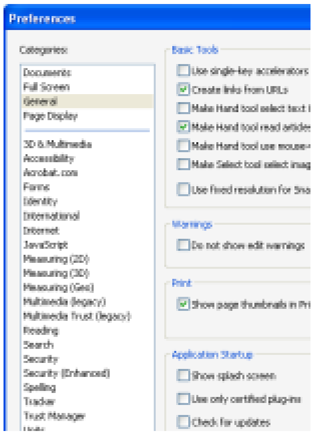
Step	Details
Step 58: To analyze PDF files, download Adobe Reader to the native host and copy it to the VM. This procedure uses Adobe Reader 9.0 as an example.	1 Install Adobe Reader 9.0 in the VM. 2 Open Adobe Reader and click **Accept**.  Adobe Reader - License Agreement Press the Accept button to agree to the License Agreement and continue. ADOBE SYSTEMS INCORPORATED Warranty Disclaimer and Software License Agreement. THIS DOCUMENT INCLUDES WARRANTY INFORMATION (PART I) AND A LICENSE AGREEM THE USE OF ADOBE SOFTWARE (PART II). PART I. WARRANTY DISCLAIMER. 3 a In Adobe Reader, select **Edit** | **Preferences** | **General** and deselect **Check for updates.** b In Adobe Reader, select **Help** | **Check for updates** | **Preferences** and deselect **Adobe Updates.**  Preferences Categories: Documents Full Screen General Page Display 3D & Multimedia Accessibility Acrobat.com Forms Identity International Internet JavaScript Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Reading Search Security Security (Enhanced) Spelling Tracker Trust Manager Basic Tools □ Use single-key accelerators ☑ Create links from URLs □ Make Hand tool select text ☑ Make Hand tool read article □ Make Hand tool use mouse- □ Make Select tool select imag □ Use fixed resolution for Sna Warnings □ Do not show edit warnings Print ☑ Show page thumbnails in Pri Application Startup □ Show splash screen □ Use only certified plug-ins □ Check for updates
Step 59: Download the following on to the native host and then install them on the VM.	1 Download Microsoft Visual C++ 2005 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=3387and install it. 2 Download Microsoft Visual C++ 2008 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5582and install it. 3 Download Microsoft Visual C++ 2010 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5555and install it. 4 Download Microsoft .NET Framework 2.0 Service Pack 2 (x86 version) from http://www.microsoft.com/en-us/download/details.aspx?id=1639and install it.
Step 60: To analyze JAR files, download and install Java Runtime Environment.	1 Goto https://community.mcafee.com/docs/DOC-6858. 2 Refer **Java installation guidance.docx**.

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

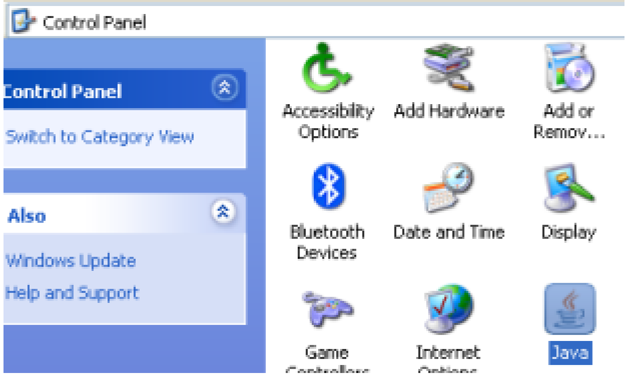
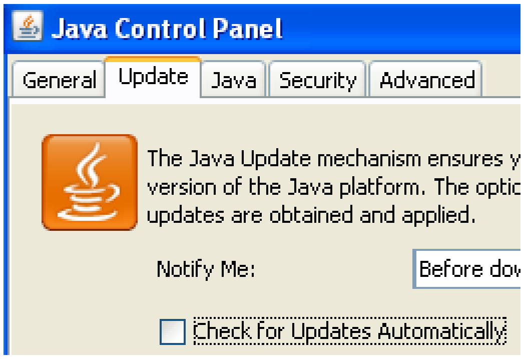
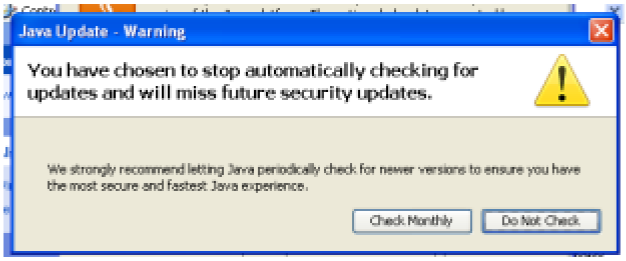
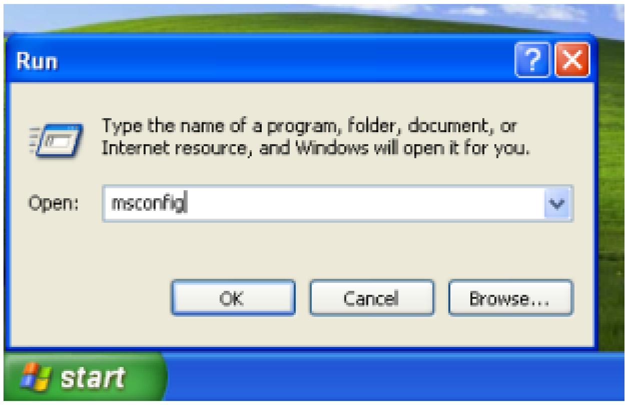
Step	Details
Step 61: Open Java in the Control Panel.	 Control Panel Control Panel Switch to Category View Also Windows Update Help and Support Accessibility Options Add Hardware Add or Remov... Bluetooth Devices Date and Time Display Game Controllers Internet Options Java
Step 62: In the **Update** tab, deselect **Check for Updates Automatically.**	 Java Control Panel General Update Java Security Advanced The Java Update mechanism ensures y version of the Java platform. The optic updates are obtained and applied. Notify Me: Before dov □ Check for Updates Automatically
Step 63: In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel.	 You have chosen to stop automatically checking for updates and will miss future security updates. We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.
Step 64: In the Windows Run dialog, enter `msconfig`.	 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: msconfig

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

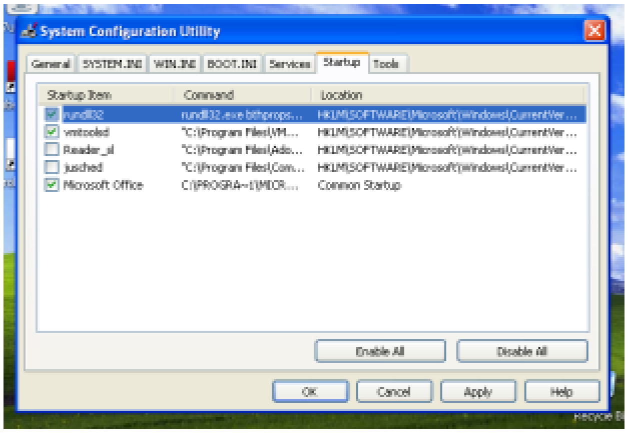
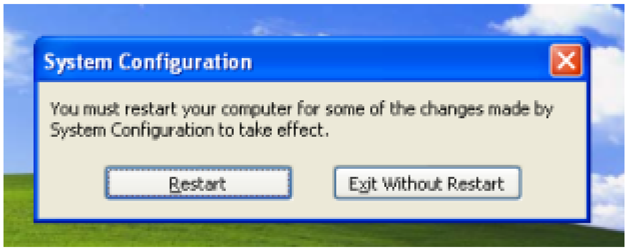
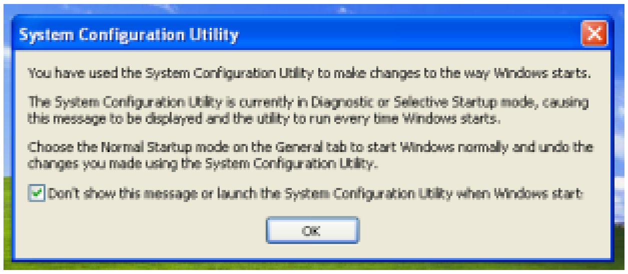
Step	Details
Step 65: In the System Configuration utility, go to the **Startup** tab.	 System Configuration Utility General SYSTEM.INI WIN.INI BOOT.INI Services Startup Tools Enable All Disable All OK Cancel Apply Help Startup Item / Command / Location ☑ rundll32 — rundll32.exe bthprops... — HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☑ vmtoolsd — "C:\Program Files\VM... — HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☐ Reader_sl — "C:\Program Files\Ado... — HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☐ jusched — "C:\Program Files\Com... — HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☑ Microsoft Office — C:\PROGRA~1\MICR... — Common Startup Deselect *reader_sl* and *jusched* and then click **OK**.
Step 66: In the **System Configuration** dialog, click **Restart**.	 You must restart your computer for some of the changes made by System Configuration to take effect.
Step 67: In the **System Configuration Utility** dialog, select **Don't show this message or launch the System Configuration Utility when Windows start** and click **OK**.	 You have used the System Configuration Utility to make changes to the way Windows starts. The System Configuration Utility is currently in Diagnostic or Selective Startup mode, causing this message to be displayed and the utility to run every time Windows starts. Choose the Normal Startup mode on the General tab to start Windows normally and undo the changes you made using the System Configuration Utility. ☑ Don't show this message or launch the System Configuration Utility when Windows start

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

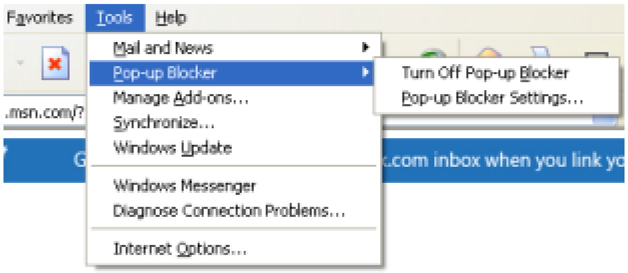
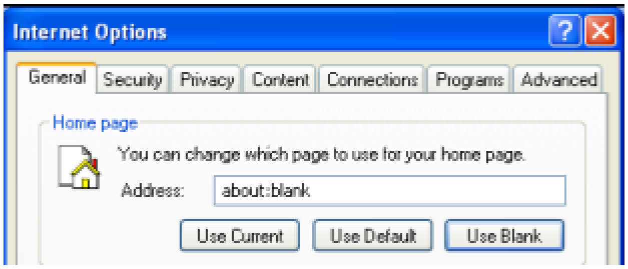
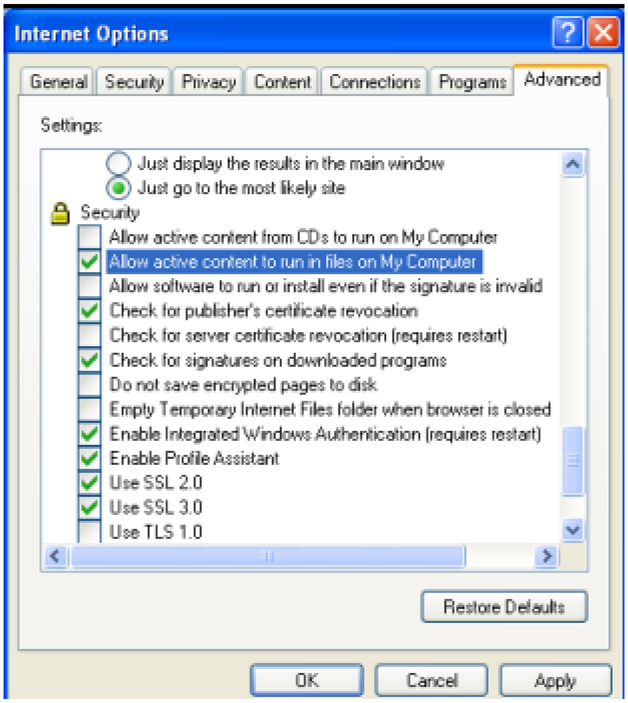
Step	Details
Step 68: Open the default browser and set it up for malware analysis. This procedure uses Internet Explorer as an example.	1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** | **Pop-up Blocker** | **Turn on Pop-up Blocker.**  Favorites Tools Help Mail and News Pop-up Blocker Manage Add-ons... Synchronize... Windows Update Windows Messenger Diagnose Connection Problems... Internet Options... Turn Off Pop-up Blocker Pop-up Blocker Settings... .msn.com/? .com inbox when you link yo 2 Select **Tools** | **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.  Internet Options General Security Privacy Content Connections Programs Advanced Home page Use Current Use Default Use Blank You can change which page to use for your home page. Address: about:blank 3 Go to the **Advanced** tab of the Internet Options and locate **Security.** 4 Select **Allow active content to run in files on My Computer.**

Table 5-2 Create a VMDK file from Windows XP SP2 or SP3 ISO image. *(continued)*

Step	Details
	 Internet Options General Security Privacy Content Connections Programs Advanced Restore Defaults OK Cancel Apply Settings: ○ Just display the results in the main window ● Just go to the most likely site Security ☐ Allow active content from CDs to run on My Computer ☑ Allow active content to run in files on My Computer ☐ Allow software to run or install even if the signature is invalid ☑ Check for publisher's certificate revocation ☐ Check for server certificate revocation (requires restart) ☑ Check for signatures on downloaded programs ☐ Do not save encrypted pages to disk ☐ Empty Temporary Internet Files folder when browser is closed ☑ Enable Integrated Windows Authentication (requires restart) ☑ Enable Profile Assistant ☑ Use SSL 2.0 ☑ Use SSL 3.0 ☐ Use TLS 1.0 5 Click **OK**.
Step 69: To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.	1 Goto https://community.mcafee.com/docs/DOC-6859. 2 Refer **Adobe flash player installation guidance.docx**.
Step 70: Shut down virtualMachineImage by selecting **Start | Shut down**.	
Step 71: Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk`	

Create a VMDK file for Windows 2003 Server

Before you begin

- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure that you have the ISO image of Windows 2003 Server SP1 or SP2 for which you need to create the VMDK file. Only Windows 2003 Server Enterprise edition is supported.
- Make sure you have the license key for the operating system.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image

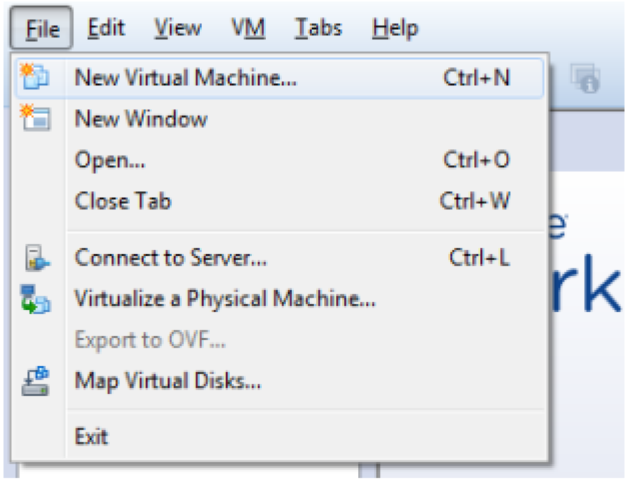
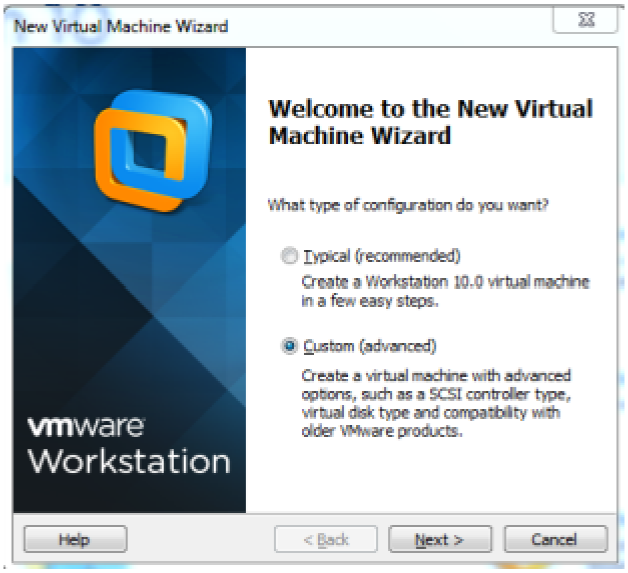
Step	Details
Step 1: Start the VMware Workstation.	This procedure uses VMware Workstation 10 as an example.
Step 2: In the VMware Workstation page, select **File | New Virtual Machine.**	 File Edit View VM Tabs Help New Virtual Machine... Ctrl+N New Window Open... Ctrl+O Close Tab Ctrl+W Connect to Server... Ctrl+L Virtualize a Physical Machine... Export to OVF... Map Virtual Disks... Exit
Step 3: In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.**	 New Virtual Machine Wizard **Welcome to the New Virtual Machine Wizard** What type of configuration do you want? ○ Typical (recommended) Create a Workstation 10.0 virtual machine in a few easy steps. ● Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

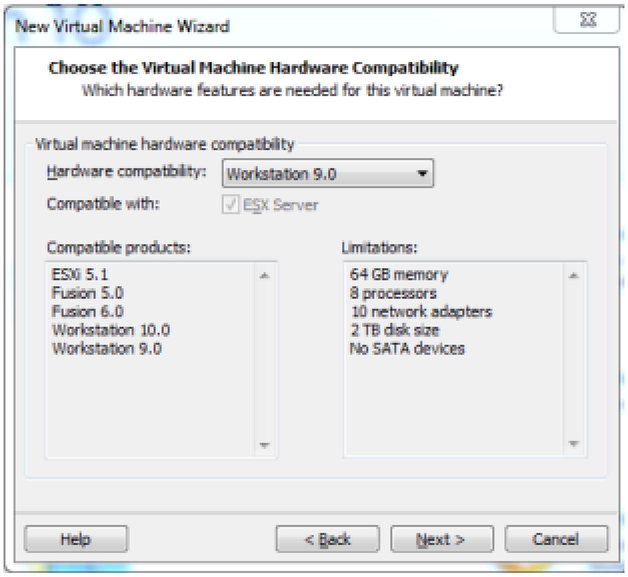
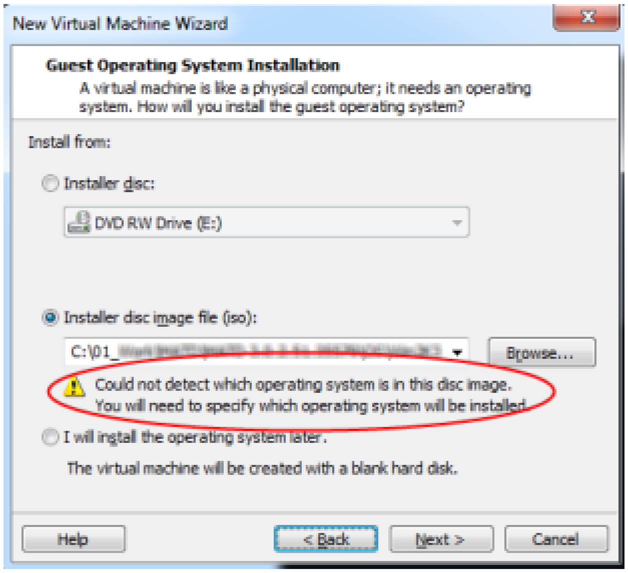
Step	Details
Step 4: In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next**.	 New Virtual Machine Wizard **Choose the Virtual Machine Hardware Compatibility** Which hardware features are needed for this virtual machine? Virtual machine hardware compatibility Hardware compatibility: Workstation 9.0 Compatible with: ☑ ESX Server Compatible products: ESXi 5.1, Fusion 5.0, Fusion 6.0, Workstation 10.0, Workstation 9.0 Limitations: 64 GB memory, 8 processors, 10 network adapters, 2 TB disk size, No SATA devices
Step 5: In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next**.	 New Virtual Machine Wizard **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: ○ Installer disc: DVD RW Drive (E:) ● Installer disc image file (iso): C:\01_[redacted] ⚠ Could not detect which operating system is in this disc image. You will need to specify which operating system will be installed. ○ I will install the operating system later. The virtual machine will be created with a blank hard disk.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

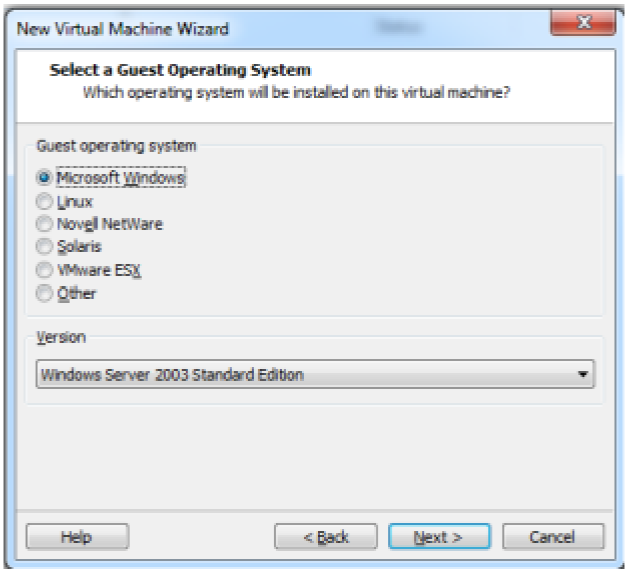
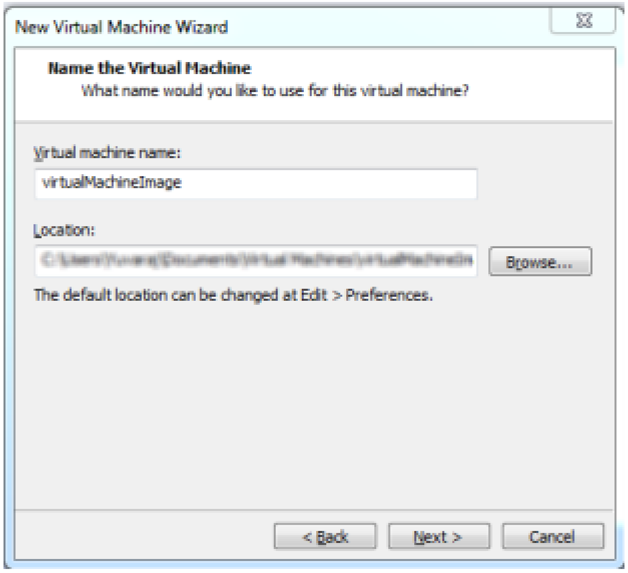
Step	Details
Step 6: In the **Select a Guest Operating System** window, select the corresponding version.	 New Virtual Machine Wizard **Select a Guest Operating System** Which operating system will be installed on this virtual machine? Guest operating system ● Microsoft Windows ○ Linux ○ Novell NetWare ○ Solaris ○ VMware ESX ○ Other Version Windows Server 2003 Standard Edition
Step 7: Enter the information in the **Name the Virtual Machine** window and then click **Next**.	• **Virtual Machine name** — You must enter `virtualMachineImage` as the name. • **Location** — Browse and select the folder where you want to create the VMDK file.  New Virtual Machine Wizard **Name the Virtual Machine** What name would you like to use for this virtual machine? Virtual machine name: virtualMachineImage Location: [redacted] The default location can be changed at Edit > Preferences.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

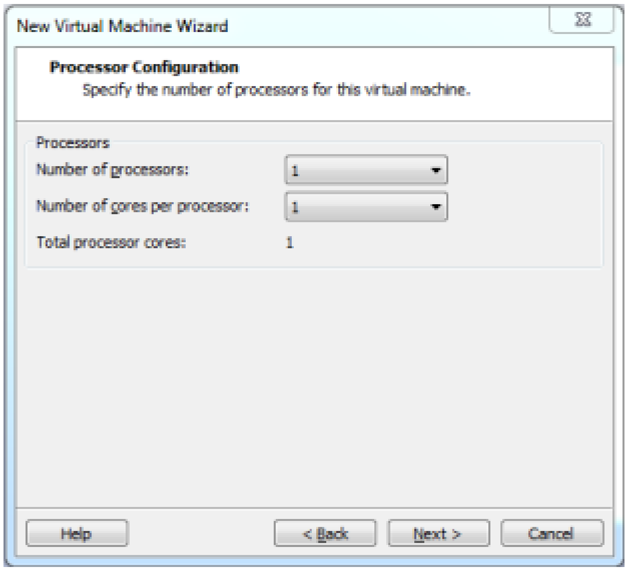
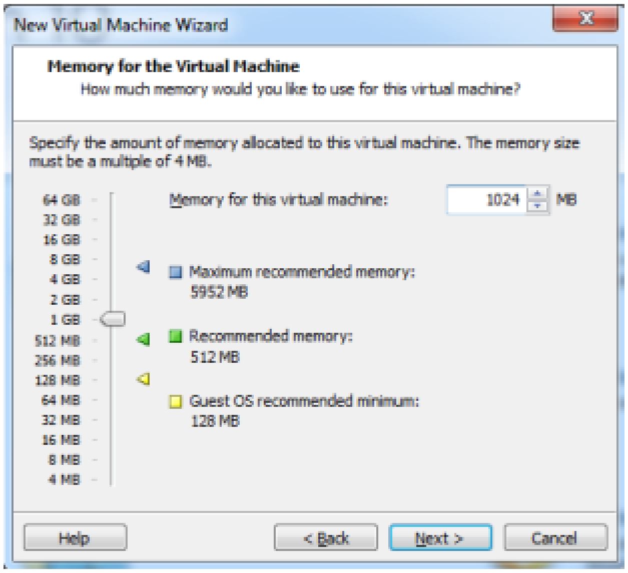
Step	Details
Step 8: In the **Processor Configuration** window, leave the default values and click **Next**.	 New Virtual Machine Wizard **Processor Configuration** Specify the number of processors for this virtual machine. Processors Number of processors: 1 Number of cores per processor: 1 Total processor cores: 1
Step 9: In the **Memory for the Virtual Machine** window, set 1024 MB as the memory.	 New Virtual Machine Wizard **Memory for the Virtual Machine** How much memory would you like to use for this virtual machine? Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB. Memory for this virtual machine: 1024 MB Maximum recommended memory: 5952 MB Recommended memory: 512 MB Guest OS recommended minimum: 128 MB 64 GB 32 GB 16 GB 8 GB 4 GB 2 GB 1 GB 512 MB 256 MB 128 MB 64 MB 32 MB 16 MB 8 MB 4 MB Help < Back Next > Cancel

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

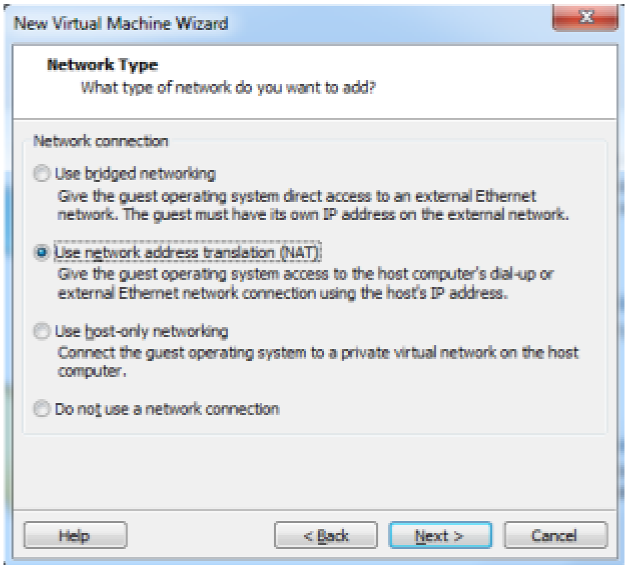
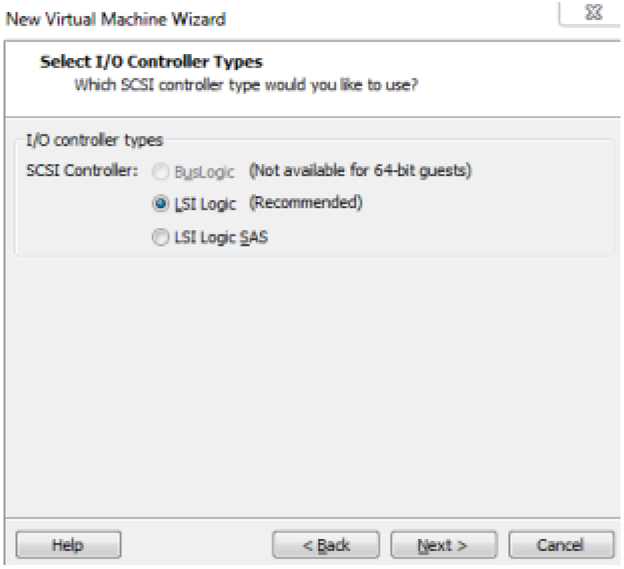
Step	Details
Step 10: In the **Network Type** window, leave the default selection.	 New Virtual Machine Wizard **Network Type** What type of network do you want to add? Network connection ○ Use bridged networking Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network. ● Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address. ○ Use host-only networking Connect the guest operating system to a private virtual network on the host computer. ○ Do not use a network connection Help < Back Next > Cancel
Step 11: In the **Select I/O Controller Types** , leave the default selection.	 New Virtual Machine Wizard **Select I/O Controller Types** Which SCSI controller type would you like to use? I/O controller types SCSI Controller: ○ BusLogic (Not available for 64-bit guests) ● LSI Logic (Recommended) ○ LSI Logic SAS Help < Back Next > Cancel

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

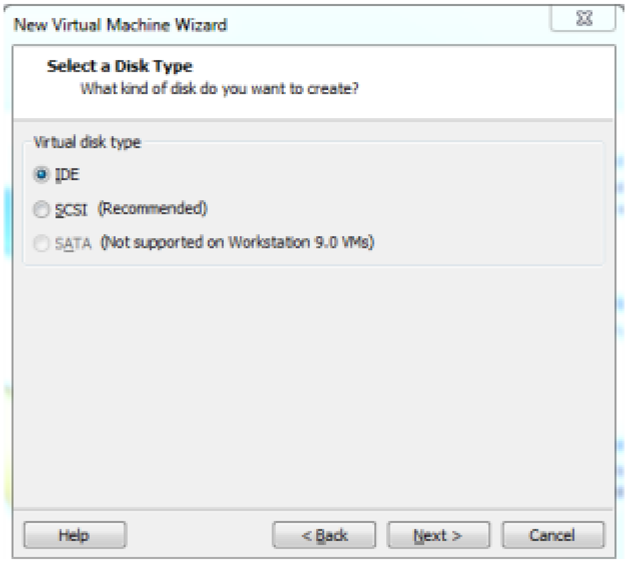
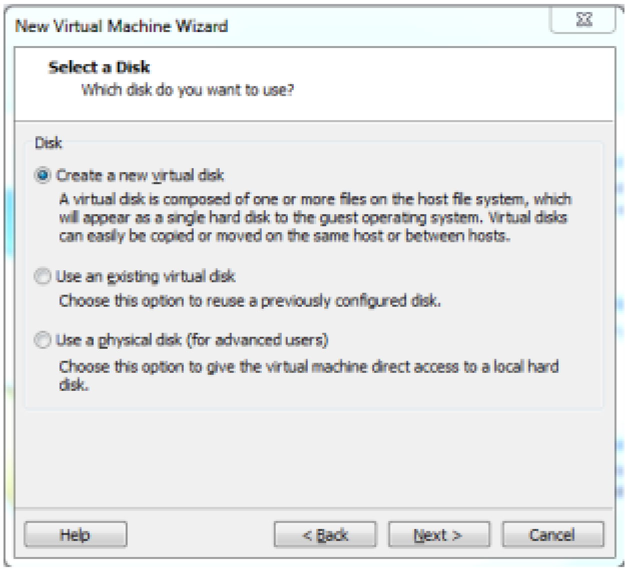
Step	Details
Step 12: In the **Select a Disk Type** page, select **IDE** and click **Next**. SCSI disks are not compatible with Advanced Threat Defense.	 New Virtual Machine Wizard **Select a Disk Type** What kind of disk do you want to create? Virtual disk type ● IDE ○ SCSI (Recommended) ○ SATA (Not supported on Workstation 9.0 VMs)
Step 13: In the **Select a Disk** window, select **Create a new virtual disk** and click **Next**.	 New Virtual Machine Wizard **Select a Disk** Which disk do you want to use? Disk ● Create a new virtual disk A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts. ○ Use an existing virtual disk Choose this option to reuse a previously configured disk. ○ Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard disk.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

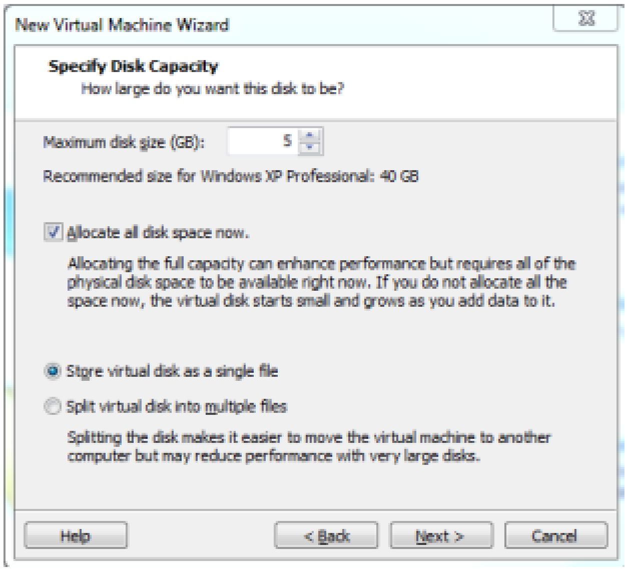
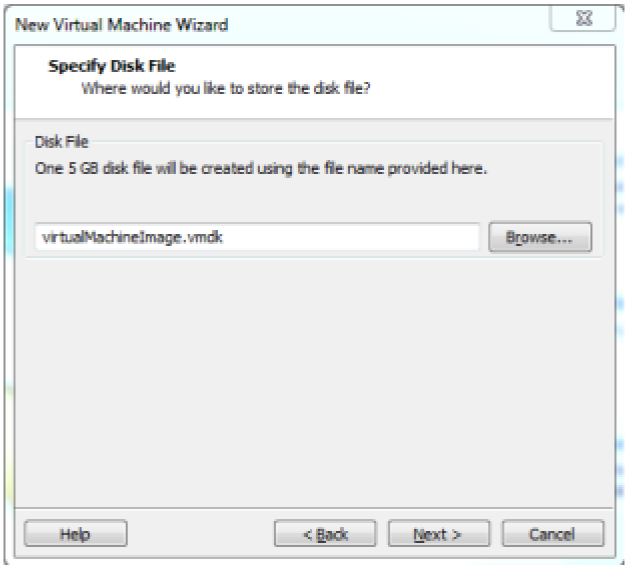
Step	Details
Step 14: Specify the details in the **Specify Disk Capacity** window and then click **Next**.	• **Maximum disk size (GB)** — For Windows 2003 Server, the maximum disk size can be 30 GB, however you must enter 5 GB for optimal performance. • Select **Allocate all disk space now**. • Select **Store virtual disk as a single file**.  New Virtual Machine Wizard **Specify Disk Capacity** How large do you want this disk to be? Maximum disk size (GB): 5 Recommended size for Windows XP Professional: 40 GB ☑ Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it. ● Store virtual disk as a single file ○ Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Step 15: In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**. If you specified a different name for **Virtual Machine name**, that name is displayed here.	 New Virtual Machine Wizard **Specify Disk File** Where would you like to store the disk file? Disk File One 5 GB disk file will be created using the file name provided here. virtualMachineImage.vmdk

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

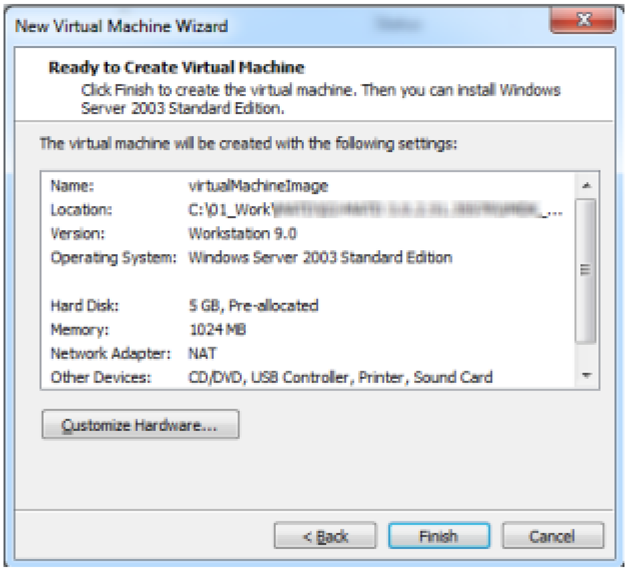
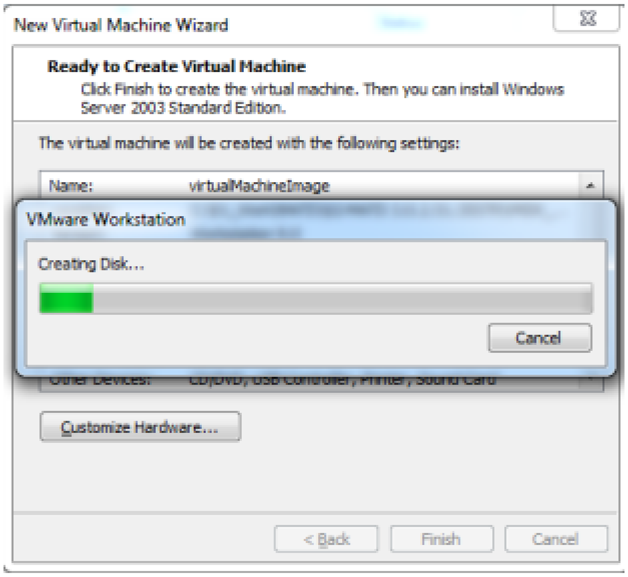
Step	Details
Step 16: Review the virtual machine creation settings and click **Finish**. This creates the virtual machine and then you must install the operating system.	 New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine. Then you can install Windows Server 2003 Standard Edition. The virtual machine will be created with the following settings: Name: virtualMachineImage Location: C:\01_Work\[redacted]_... Version: Workstation 9.0 Operating System: Windows Server 2003 Standard Edition Hard Disk: 5 GB, Pre-allocated Memory: 1024 MB Network Adapter: NAT Other Devices: CD/DVD, USB Controller, Printer, Sound Card  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine. Then you can install Windows Server 2003 Standard Edition. The virtual machine will be created with the following settings: Name: virtualMachineImage VMware Workstation Creating Disk... Other Devices: CD/DVD, USB Controller, Printer, Sound Card Cancel Customize Hardware... < Back Finish Cancel

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

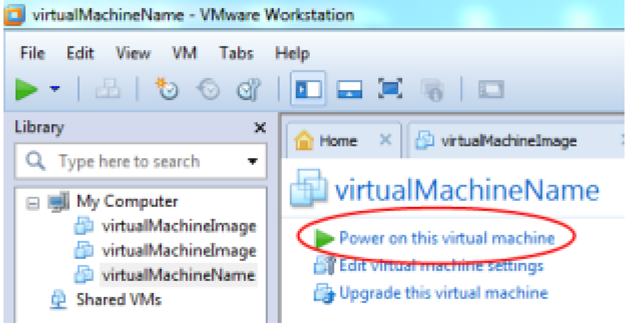
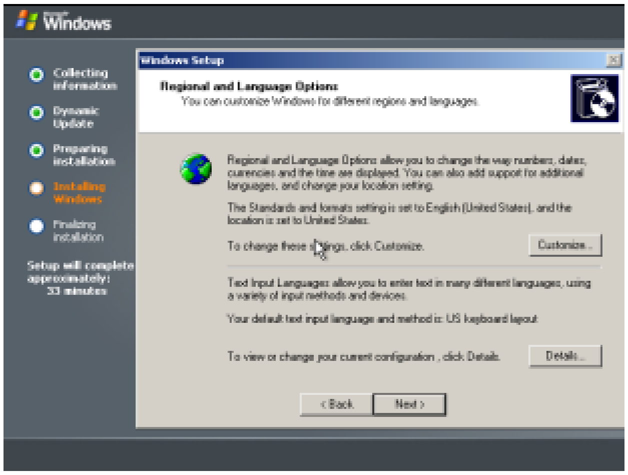
Step	Details
Step 17: In the VMware Workstation, power on the virtual machine that you just created and install Windows Server 2003 following the usual procedure. • This step might take around 30 minutes to complete. • You can use the NTFS file system to format the partition during installation. • Do not install VMware Tools. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready.	 virtualMachineName - VMware Workstation File Edit View VM Tabs Help Library Type here to search My Computer virtualMachineImage virtualMachineImage virtualMachineName Shared VMs Home virtualMachineImage virtualMachineName Power on this virtual machine Edit virtual machine settings Upgrade this virtual machine
Step 18: In the **Regional and Language Options** window, you can customize the settings.	 Windows Windows Setup Collecting information Dynamic Update Preparing installation Installing Windows Finalizing installation Setup will complete approximately: 33 minutes Customize... Details... < Back Next > **Regional and Language Options** You can customize Windows for different regions and languages. Regional and Language Options allow you to change the way numbers, dates, currencies and the time are displayed. You can also add support for additional languages, and change your location setting. The Standards and formats setting is set to English (United States), and the location is set to United States. To change these settings, click Customize. Text Input Languages allow you to enter text in many different languages, using a variety of input methods and devices. Your default text input language and method is: US keyboard layout To view or change your current configuration , click Details.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

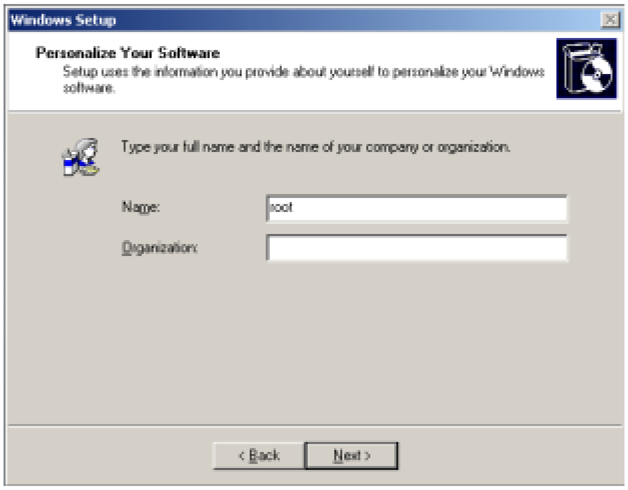
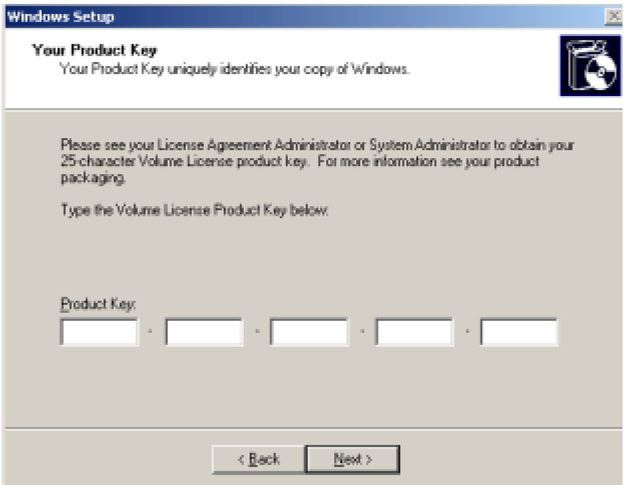
Step	Details
Step 19: Enter the following details in the **Windows Setup** window.	- **Name:** Enter `root` - **Organization:** Leave this blank and click **Next**.  **Windows Setup** **Personalize Your Software** Setup uses the information you provide about yourself to personalize your Windows software. Type your full name and the name of your company or organization. Name: root Organization:
Step 20: Enter a valid product key and click **Next**.	 **Windows Setup** **Your Product Key** Your Product Key uniquely identifies your copy of Windows. Please see your License Agreement Administrator or System Administrator to obtain your 25-character Volume License product key. For more information see your product packaging. Type the Volume License Product Key below. Product Key:

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

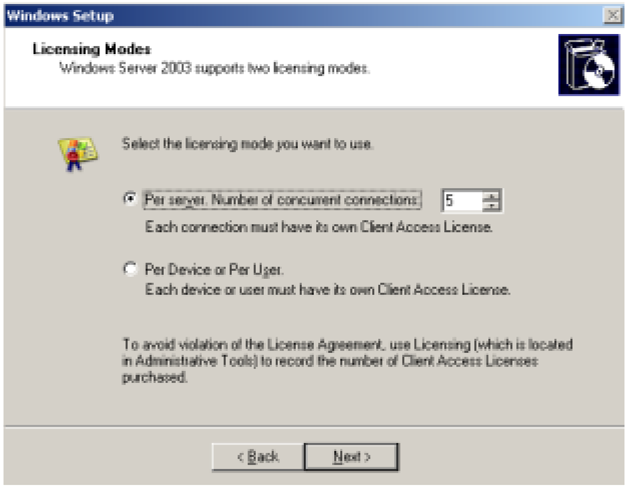
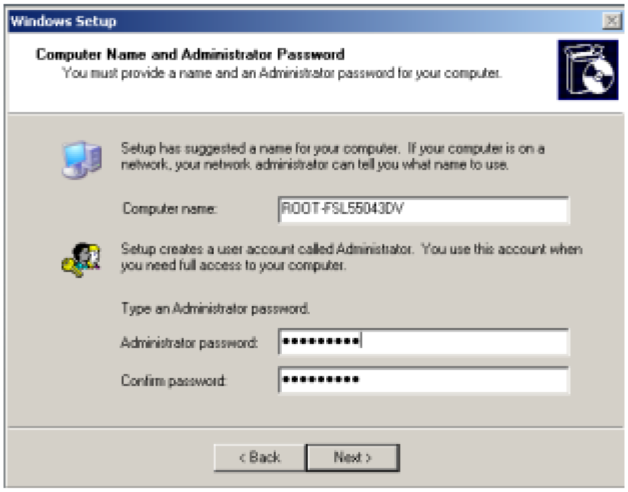
Step	Details
Step 21: Select **Per Server** licensing mode and enter the valid number of concurrent connections as per your license.	 **Licensing Modes** Windows Server 2003 supports two licensing modes. Select the licensing mode you want to use. ● Per server. Number of concurrent connections: 5 Each connection must have its own Client Access License. ○ Per Device or Per User. Each device or user must have its own Client Access License. To avoid violation of the License Agreement, use Licensing (which is located in Administrative Tools) to record the number of Client Access Licenses purchased.
Step 22: Enter the following details in the **Computer Name and Administrator Password** window.	• Computer name — leave the default value. • Administrator password — `cr@cker42` • Confirm password — `cr@cker42`  **Computer Name and Administrator Password** You must provide a name and an Administrator password for your computer. Setup has suggested a name for your computer. If your computer is on a network, your network administrator can tell you what name to use. Computer name: ROOT-FSL55043DV Setup creates a user account called Administrator. You use this account when you need full access to your computer. Type an Administrator password. Administrator password: •••••••••• Confirm password: ••••••••••

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

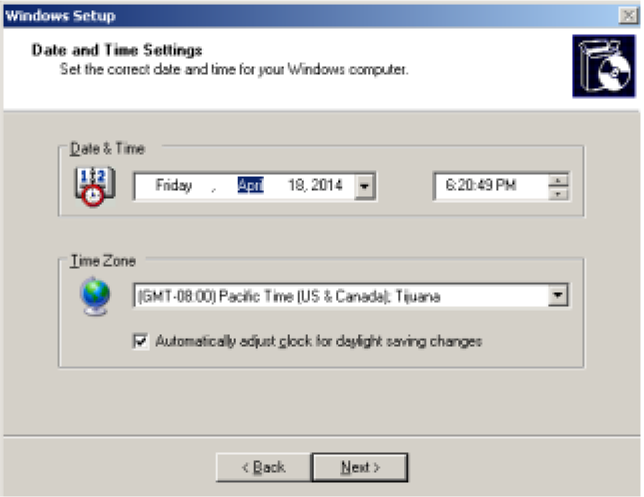
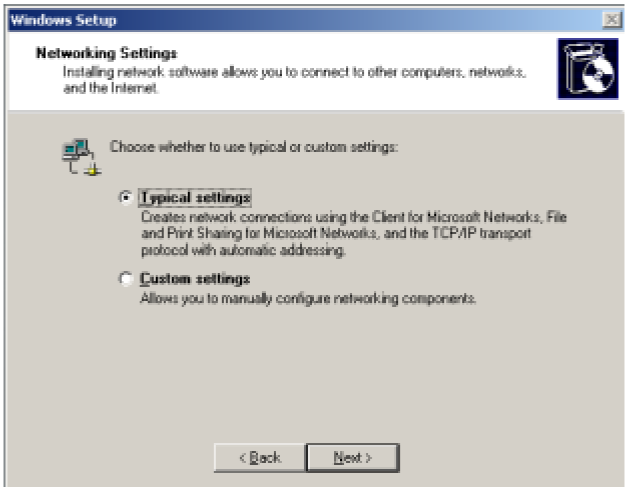
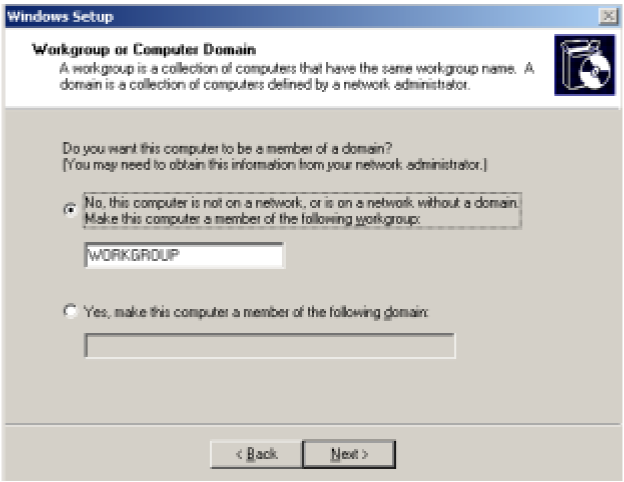
Step	Details
Step 23: Click **Next** in the **Date and Time Settings** window.	 **Date and Time Settings** Set the correct date and time for your Windows computer. Date & Time Friday , April 18, 2014 6:20:49 PM Time Zone (GMT-08:00) Pacific Time (US & Canada); Tijuana ☑ Automatically adjust clock for daylight saving changes
Step 24: In the **Network Settings** window, leave the default values and click **Next.**	 **Networking Settings** Installing network software allows you to connect to other computers, networks, and the Internet. Choose whether to use typical or custom settings: ● **Typical settings** Creates network connections using the Client for Microsoft Networks, File and Print Sharing for Microsoft Networks, and the TCP/IP transport protocol with automatic addressing. ○ **Custom settings** Allows you to manually configure networking components.
Step 25: Leave the default values in the **Workgroup or Computer Domain** window and click **Next.**	 **Workgroup or Computer Domain** A workgroup is a collection of computers that have the same workgroup name. A domain is a collection of computers defined by a network administrator. Do you want this computer to be a member of a domain? (You may need to obtain this information from your network administrator.) ● No, this computer is not on a network, or is on a network without a domain. Make this computer a member of the following workgroup: WORKGROUP ○ Yes, make this computer a member of the following domain:

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

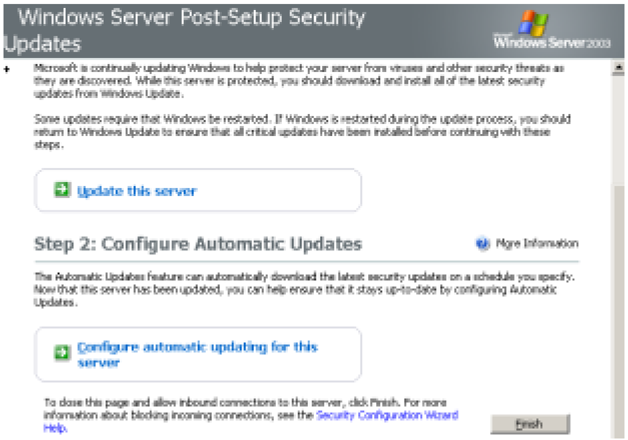
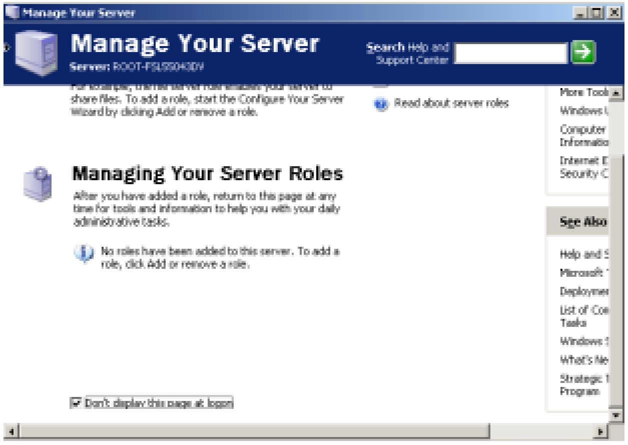
Step	Details
Step 26: Log on to the virtual machine with the following credentials.	• **User:** `administrator` • **Password:** `cr@cker42`
Step 27: If the **Windows Server Post-Setup Security Updates** page is displayed, click **Finish.**	 Windows Server Post-Setup Security Updates Microsoft is continually updating Windows to help protect your server from viruses and other security threats as they are discovered. While this server is protected, you should download and install all of the latest security updates from Windows Update. Some updates require that Windows be restarted. If Windows is restarted during the update process, you should return to Windows Update to ensure that all critical updates have been installed before continuing with these steps. Update this server Step 2: Configure Automatic Updates More Information The Automatic Updates feature can automatically download the latest security updates on a schedule you specify. Now that this server has been updated, you can help ensure that it stays up-to-date by configuring Automatic Updates. Configure automatic updating for this server To close this page and allow inbound connections to this server, click Finish. For more information about blocking incoming connections, see the Security Configuration Wizard Help. Finish
Step 28: If the **Manage Your Server** window is displayed, select **Don't Display the page at logon** and close it.	 Manage Your Server Server: ROOT-FSLS5043DV Search Help and Support Center share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role. Read about server roles Managing Your Server Roles After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks. No roles have been added to this server. To add a role, click Add or remove a role. ☑ Don't display this page at logon See Also

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

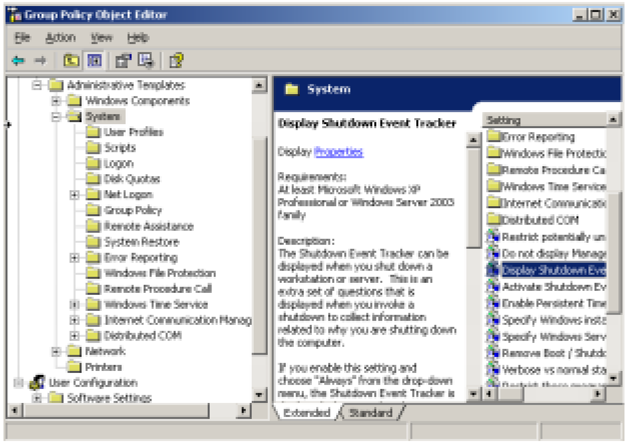
Step	Details
Step 29: Complete the following steps.	1 Select **Start** | **Run** and enter `gpedit.msc`. 2 In the **Group policy object editor** window, select **Computer Configuration** | **Administrative Templates** | **System** and double-click **Display Shutdown Event Tracker.**  Group Policy Object Editor File Action View Help Administrative Templates Windows Components System User Profiles Scripts Logon Disk Quotas Net Logon Group Policy Remote Assistance System Restore Error Reporting Windows File Protection Remote Procedure Call Windows Time Service Internet Communication Manag Distributed COM Network Printers User Configuration Software Settings System Setting Error Reporting Windows File Protectic Remote Procedure Ca Windows Time Service Internet Communicatic Distributed COM Restrict potentially un Do not display Manage Display Shutdown Eve Activate Shutdown Ev Enable Persistent Time Specify Windows insta Specify Windows Serv Remove Boot / Shutdc Verbose vs normal sta Extended Standard Display Shutdown Event Tracker Display Properties Requirements: At least Microsoft Windows XP Professional or Windows Server 2003 family Description: The Shutdown Event Tracker can be displayed when you shut down a workstation or server. This is an extra set of questions that is displayed when you invoke a shutdown to collect information related to why you are shutting down the computer. If you enable this setting and choose "Always" from the drop-down menu, the Shutdown Event Tracker is 3 Select **Disabled** and click **OK.** 4 Close the **Group policy object editor** window.
Step 30: Complete the following steps only for Windows Server 2003 SP1. For Windows Server 2003 SP2, you must not execute this step.	1 Go to http://support.microsoft.com/hotfix/KBHotfix.aspx?kbnum=899260&kbln=en-us and install the hotfix corresponding to your version of Windows Server 2003. 2 Restart the computer. 3 In the Windows command prompt, enter `tlntsvr /service` and press Enter.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

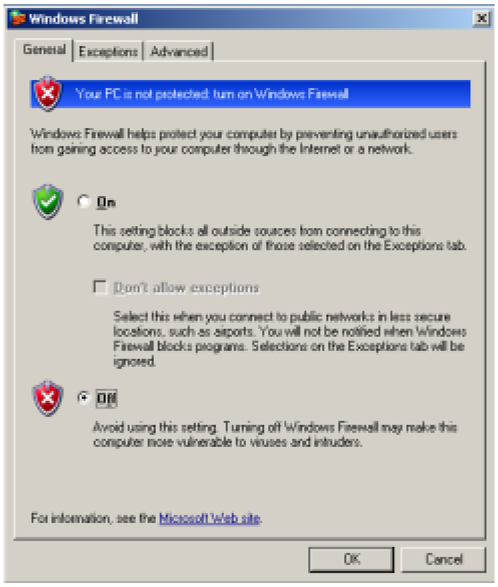
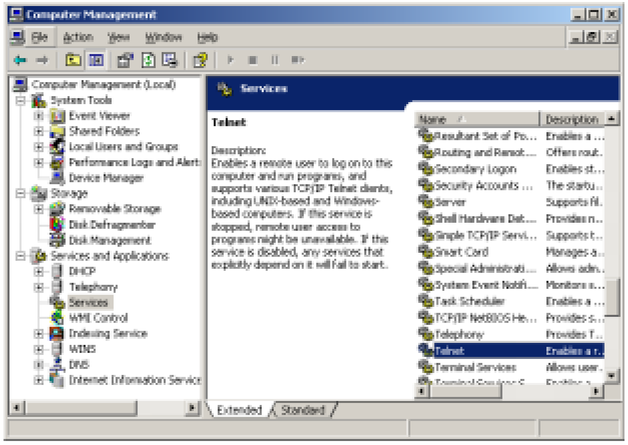
Step	Details
Step 31: In the virtualMachineImage, select **Start** | **Control Panel** | **Windows Firewall** | **OFF**.	 Your PC is not protected: turn on Windows Firewall Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network. ○ On This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab. □ Don't allow exceptions Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored. ● Off Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders. For information, see the Microsoft Web site.
Step 32: Click **Start** and right-click **My Computer**. Then select **Manage** | **Services and Applications** | **Services.** Then, double-click **Telnet.**	 Computer Management File Action View Window Help Computer Management (Local) System Tools Event Viewer Shared Folders Local Users and Groups Performance Logs and Alert: Device Manager Storage Removable Storage Disk Defragmenter Disk Management Services and Applications DHCP Telephony Services WMI Control Indexing Service WINS DNS Internet Information Servic Services **Telnet** Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. Name – Description Resultant Set of Po... – Enables a ... Routing and Remot... – Offers rout. Secondary Logon – Enables st... Security Accounts ... – The startu... Server – Supports fil. Shell Hardware Det... – Provides n... Simple TCP/IP Servi... – Supports t... Smart Card – Manages a... Special Administrati... – Allows adn.. System Event Notifi... – Monitors s... Task Scheduler – Enables a ... TCP/IP NetBIOS He... – Provides s... Telephony – Provides T... Telnet – Enables a r.. Terminal Services – Allows user.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

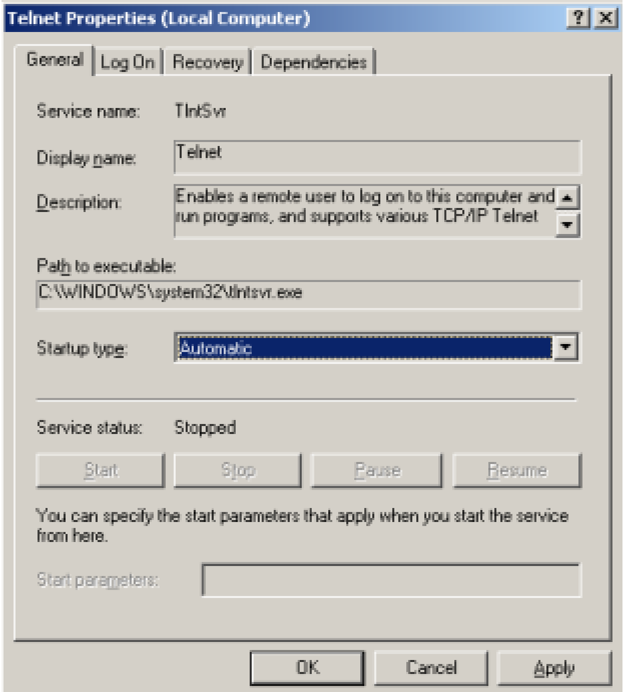
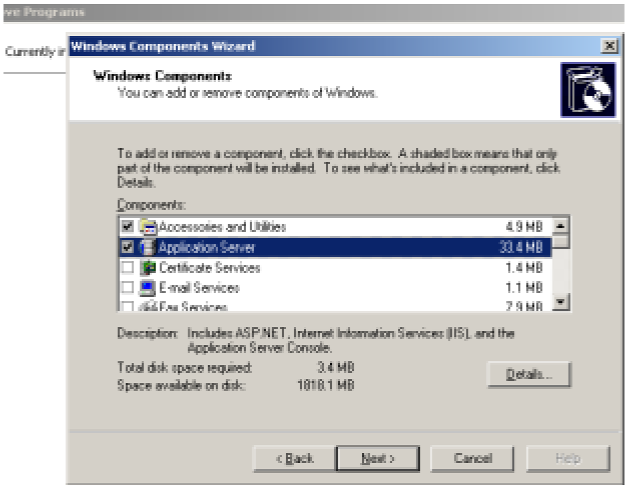
Step	Details
Step 33: In the **Telnet Properties(Local Computer)** window, you must select **Automatic** from the **Startup type** drop-down list. Then select **Apply** | **Start** | **OK**.	 Telnet Properties (Local Computer) General | Log On | Recovery | Dependencies Service name: TlntSvr Display name: Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet Path to executable: C:\WINDOWS\system32\tlntsvr.exe Startup type: Automatic Service status: Stopped Start | Stop | Pause | Resume You can specify the start parameters that apply when you start the service from here. Start parameters: OK | Cancel | Apply
Step 34: Enable FTP on the VM.	1 In the virtualMachineImage, select **Start** | **Control Panel** | **Add or remove Programs** | **Add/Remove Windows components.**  Windows Components Wizard Windows Components You can add or remove components of Windows. To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Components: ☑ Accessories and Utilities 4.9 MB ☑ Application Server 33.4 MB ☐ Certificate Services 1.4 MB ☐ E-mail Services 1.1 MB ☐ Fax Services 7.9 MB Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console. Total disk space required: 3.4 MB Space available on disk: 1818.1 MB Details... < Back | Next > | Cancel | Help 2 Double-click **Application Server.** 3 Double-click **Internet Information Services(IIS)**

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

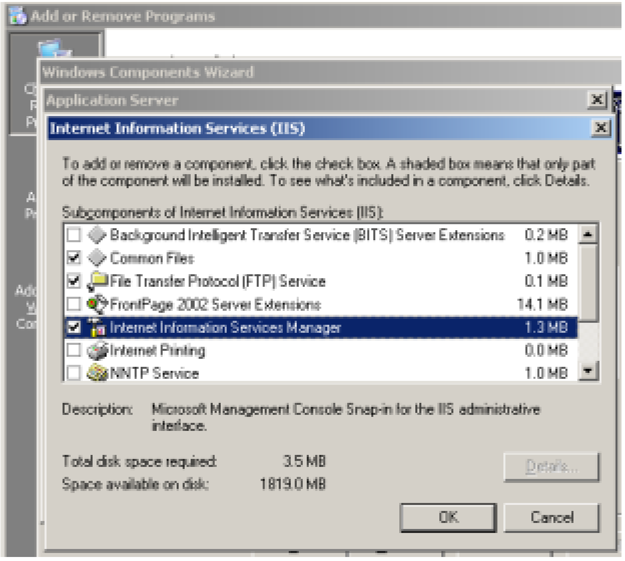
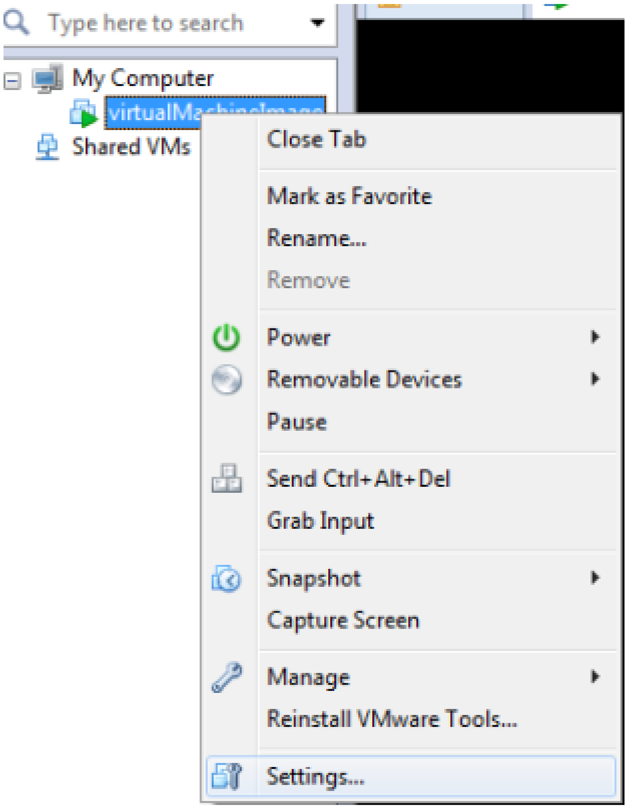
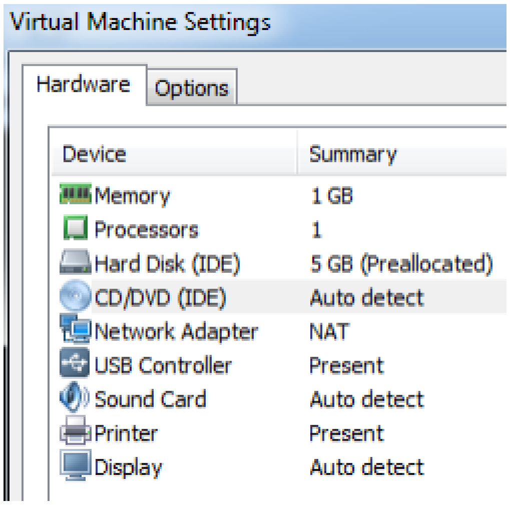
Step	Details
Step 35: In the **Internet Information Services(IIS)** pop-up window, complete the following.	1 Select **Common Files**. 2 Select **File Transfer Protocol (FTP) Service**. 3 Select **Internet Information Services Manager**, click **OK**, and then click **Next** in the **Windows Components Wizard.**  Add or Remove Programs Windows Components Wizard Application Server Internet Information Services (IIS) To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details. Subcomponents of Internet Information Services (IIS): □ Background Intelligent Transfer Service (BITS) Server Extensions 0.2 MB ☑ Common Files 1.0 MB ☑ File Transfer Protocol (FTP) Service 0.1 MB □ FrontPage 2002 Server Extensions 14.1 MB ☑ Internet Information Services Manager 1.3 MB □ Internet Printing 0.0 MB □ NNTP Service 1.0 MB Description: Microsoft Management Console Snap-in for the IIS administrative interface. Total disk space required: 3.5 MB Space available on disk: 1819.0 MB

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

<table>
<tr><th>Step</th><th>Details</th></tr>
<tr><td><b>Step 36:</b> In the VMware Workstation, right-click on the VM, which in this example is virtualMachineImage. Then, select <b>Settings</b>.</td><td>
 </td></tr>
<tr><td><b>Step 37:</b> In the Virtual Machine Settings window, select <b>CD/DVD (IDE)</b>.</td><td>

<table>
<tr><th>Device</th><th>Summary</th></tr>
<tr><td>Memory</td><td>1 GB</td></tr>
<tr><td>Processors</td><td>1</td></tr>
<tr><td>Hard Disk (IDE)</td><td>5 GB (Preallocated)</td></tr>
<tr><td>CD/DVD (IDE)</td><td>Auto detect</td></tr>
<tr><td>Network Adapter</td><td>NAT</td></tr>
<tr><td>USB Controller</td><td>Present</td></tr>
<tr><td>Sound Card</td><td>Auto detect</td></tr>
<tr><td>Printer</td><td>Present</td></tr>
<tr><td>Display</td><td>Auto detect</td></tr>
</table></td></tr>
</table>

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

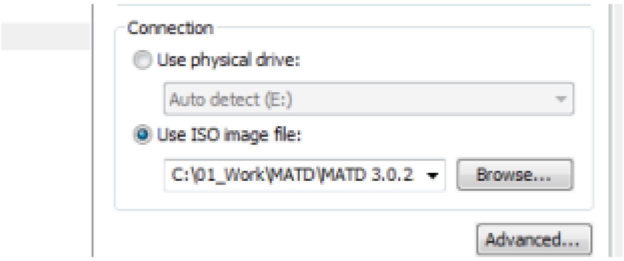
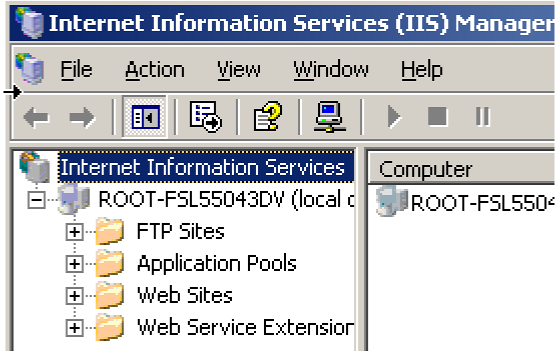
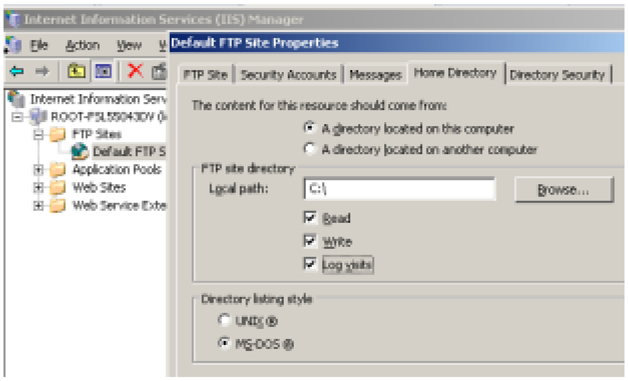
Step	Details
Step 38: In the **Use ISO image file** field, browse to the ISO file that you used and press **OK**. Close Windows Explorer, if it opens.	 Connection ○ Use physical drive: Auto detect (E:) ● Use ISO image file: C:\01_Work\MATD\MATD 3.0.2
Step 39: In the virtualMachineImage, select **Start** | **Control Panel** | **Administrative Tools** | **Internet Information Services (IIS) Manager.**	
Step 40: In the **Internet Information Services (IIS) Manager** window, expand + below **Internet Information Services.**	 Internet Information Services (IIS) Manager File Action View Window Help Internet Information Services ROOT-FSL55043DV (local c FTP Sites Application Pools Web Sites Web Service Extension Computer ROOT-FSL5504
Step 41: Complete the following.	1 Select **FTP Sites** and then right-click **Default FTP Sites.** 2 Select **Properties** | **Home Directory.** 3 Browse to C:\\ 4 Select **Read**. 5 Select **Write**. 6 Select **Log visits** and click **Apply** and then **OK.**  Internet Information Services (IIS) Manager File Action View Internet Information Serv ROOT-FSL55043DV (l FTP Sites Default FTP S Application Pools Web Sites Web Service Exte Default FTP Site Properties FTP Site | Security Accounts | Messages | Home Directory | Directory Security The content for this resource should come from: ● A directory located on this computer ○ A directory located on another computer FTP site directory Local path: C:\\ ☑ Read ☑ Write ☑ Log visits Directory listing style ○ UNIX ® ● MS-DOS ®

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

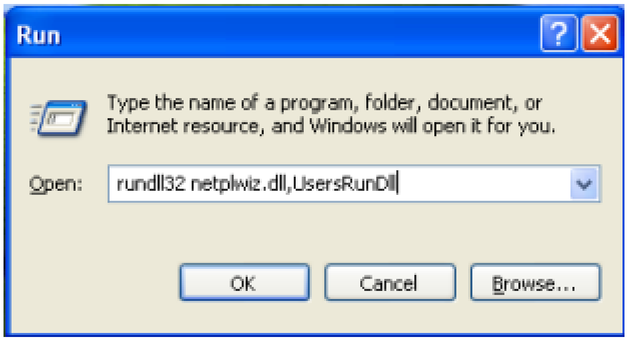
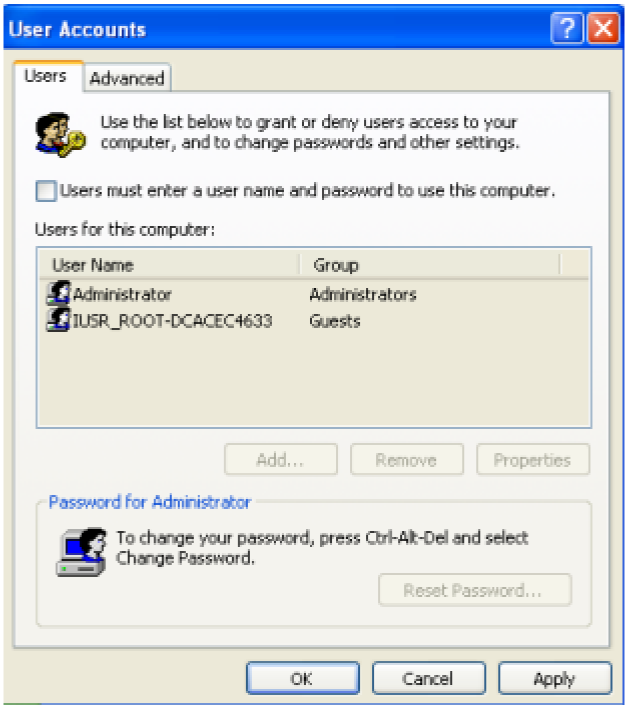
Step	Details
Step 42: Set automatic logon by selecting **Start** | **Run**, enter `rundll32 netplwiz.dll,UsersRunDll` and press **Enter**.	 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: rundll32 netplwiz.dll,UsersRunDll
Step 43: In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**.	 User Accounts Users Advanced Add... Remove Properties Reset Password... OK Cancel Apply Use the list below to grant or deny users access to your computer, and to change passwords and other settings. □ Users must enter a user name and password to use this computer. Users for this computer: User Name — Group Administrator — Administrators IUSR_ROOT-DCACEC4633 — Guests Password for Administrator To change your password, press Ctrl-Alt-Del and select Change Password.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

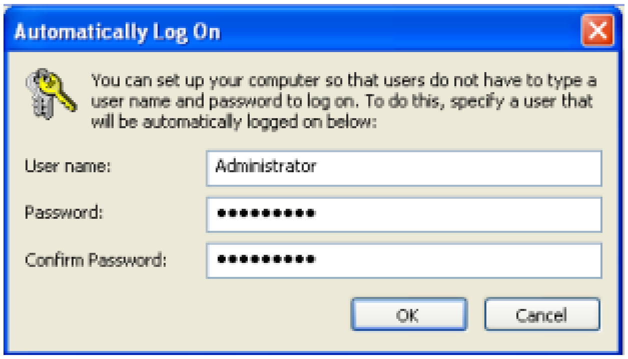
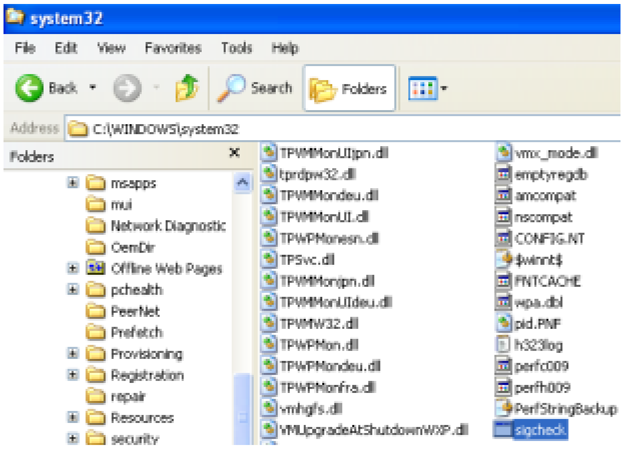
Step	Details
Step 44: In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes.	• **User name** — Enter `Administrator` • **Password** — Enter `cr@cker42` • **Confirm Password** — Enter `cr@cker42`  Automatically Log On You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below: User name: Administrator Password: ••••••••• Confirm Password: •••••••••
Step 45: Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx.	The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation.
Step 46: Extract sigcheck.zip to `C:\WINDOWS\system32` location.	 Address C:\WINDOWS\system32 system32 File Edit View Favorites Tools Help Back Search Folders Folders msapps mui Network Diagnostic OemDir Offline Web Pages pchealth PeerNet Prefetch Provisioning Registration repair Resources security TPVMMonUIjpn.dll tprdpw32.dll TPVMMondeu.dll TPVMMonUI.dll TPWPMonesn.dll TPSvc.dll TPVMMonjpn.dll TPVMMonUIdeu.dll TPVMW32.dll TPWPMon.dll TPWPMondeu.dll TPWPMonfra.dll vmhgfs.dll VMUpgradeAtShutdownWXP.dll vmx_mode.dll emptyregdb amcompat nscompat CONFIG.NT $winnt$ FNTCACHE wpa.dbl pid.PNF h323log perfc009 perfh009 PerfStringBackup sigcheck
Step 47: In Windows Explorer, go to C:\ WINDOWS\system32 and double-click **sigcheck.exe**.	
Step 48: If prompted, click **Run** in the warning message.	

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

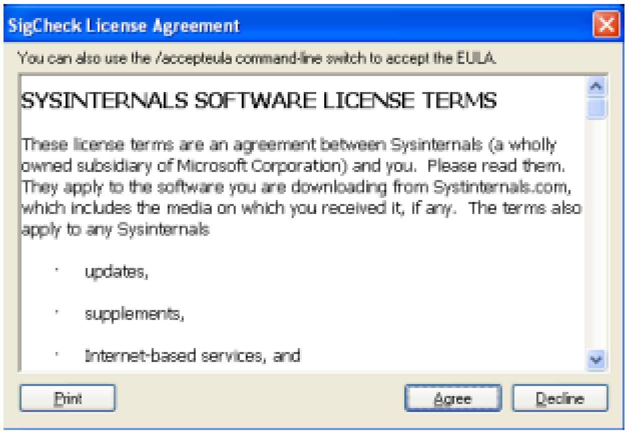
Step	Details
Step 49: Click **Agree** for **Sigcheck License Agreement**. After you click on **Agree**, no confirmation message is displayed.	 SigCheck License Agreement You can also use the /accepteula command-line switch to accept the EULA. SYSINTERNALS SOFTWARE LICENSE TERMS These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals · updates, · supplements, · Internet-based services, and
Step 50: Run the MergeIDE batch file on the VM.	1 Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM. 2 Extract MergeIDE.zip and run the MergeIDE batch file in the VM. 3 If prompted, select **Run** in the warning message. 4 Close Windows Explorer.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

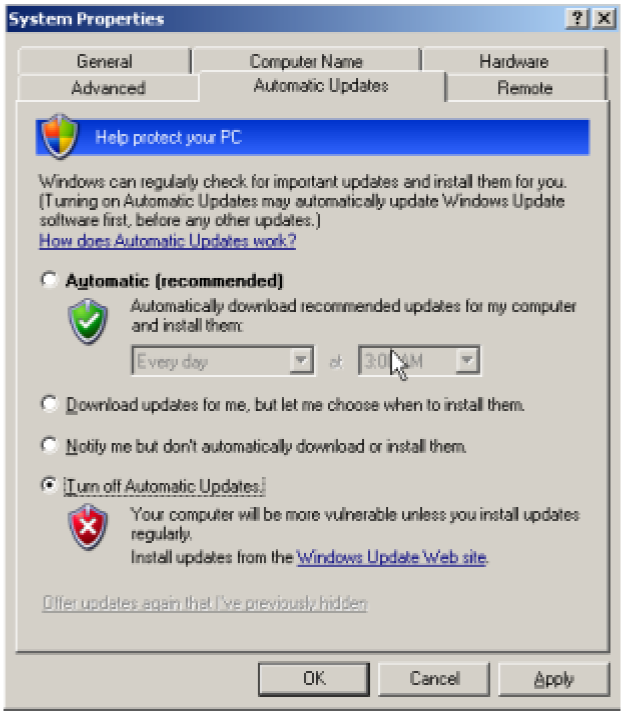
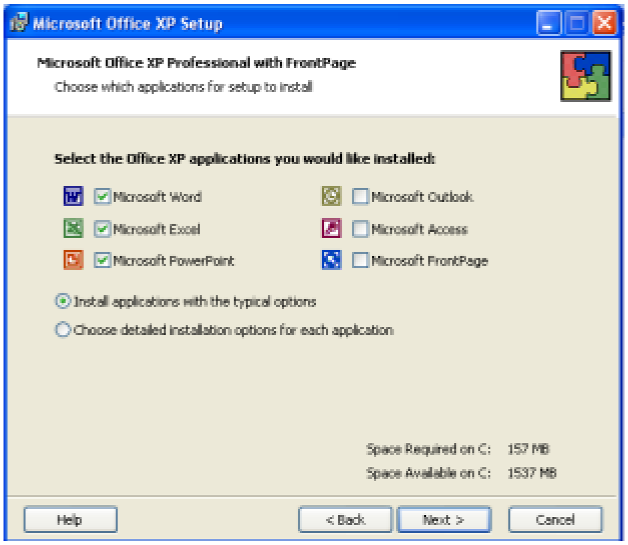
Step	Details
Step 51: Disable Windows updates.	1 Select **Start** | **Control Panel** | **System** | **Automatic Updates.** 2 In the **System Properties** window, select **Turn off Automatic Updates.** System Properties General | Computer Name | Hardware | Advanced | Automatic Updates | Remote Help protect your PC Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.) How does Automatic Updates work? ○ Automatic (recommended) Automatically download recommended updates for my computer and install them: Every day at 3:00 AM ○ Download updates for me, but let me choose when to install them. ○ Notify me but don't automatically download or install them. ● Turn off Automatic Updates. Your computer will be more vulnerable unless you install updates regularly. Install updates from the Windows Update Web site. Offer updates again that I've previously hidden OK | Cancel | Apply 3 Click **Apply** and then **OK.**
Step 52: To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine.	Microsoft Office XP Setup Microsoft Office XP Professional with FrontPage Choose which applications for setup to install Select the Office XP applications you would like installed: ☑ Microsoft Word ☐ Microsoft Outlook ☑ Microsoft Excel ☐ Microsoft Access ☑ Microsoft PowerPoint ☐ Microsoft FrontPage ● Install applications with the typical options ○ Choose detailed installation options for each application Space Required on C: 157 MB Space Available on C: 1537 MB Help | < Back | Next > | Cancel

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

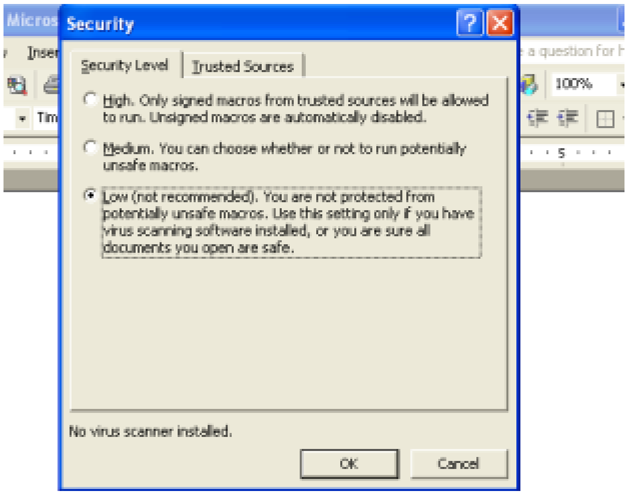
Step	Details
Step 53: Lower the security to run macros for the Office applications.	- Open Microsoft Word 2003 and select **Tools** | **Macro** | **Security** and then select **Low** and click **OK**.  Security Security Level Trusted Sources OK Cancel ○ High. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled. ○ Medium. You can choose whether or not to run potentially unsafe macros. ● Low (not recommended). You are not protected from potentially unsafe macros. Use this setting only if you have virus scanning software installed, or you are sure all documents you open are safe. No virus scanner installed. - Similarly lower the macro security for Microsoft Excel and Powerpoint.
Step 54: You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed. Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine.	

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

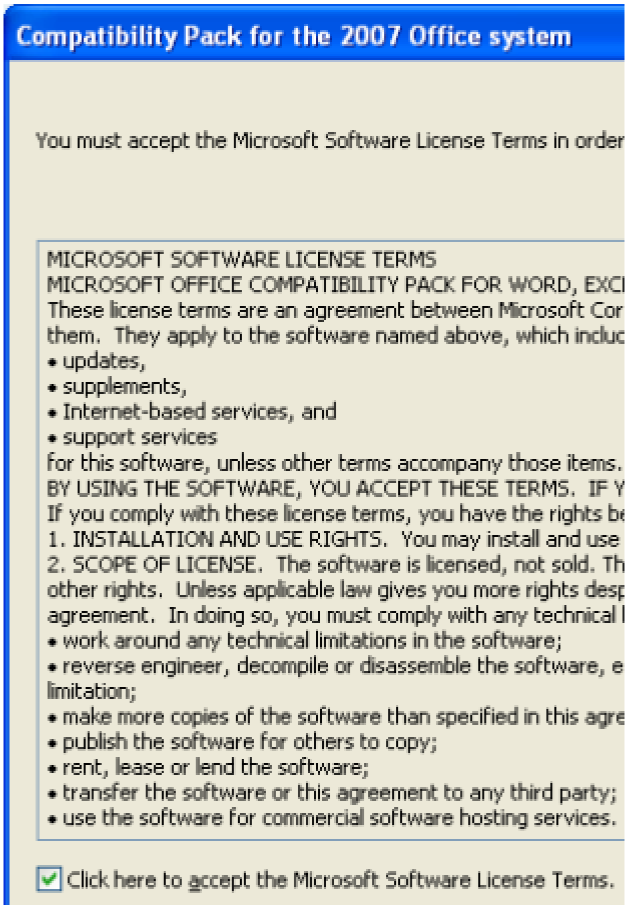
Step	Details
Step 55: In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **OK**.	 Compatibility Pack for the 2007 Office system You must accept the Microsoft Software License Terms in order MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT OFFICE COMPATIBILITY PACK FOR WORD, EXCI These license terms are an agreement between Microsoft Cor them. They apply to the software named above, which incluc • updates, • supplements, • Internet-based services, and • support services for this software, unless other terms accompany those items. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF Y If you comply with these license terms, you have the rights be 1. INSTALLATION AND USE RIGHTS. You may install and use 2. SCOPE OF LICENSE. The software is licensed, not sold. Th other rights. Unless applicable law gives you more rights desp agreement. In doing so, you must comply with any technical l • work around any technical limitations in the software; • reverse engineer, decompile or disassemble the software, e limitation; • make more copies of the software than specified in this agre • publish the software for others to copy; • rent, lease or lend the software; • transfer the software or this agreement to any third party; • use the software for commercial software hosting services. ☑ Click here to accept the Microsoft Software License Terms.

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

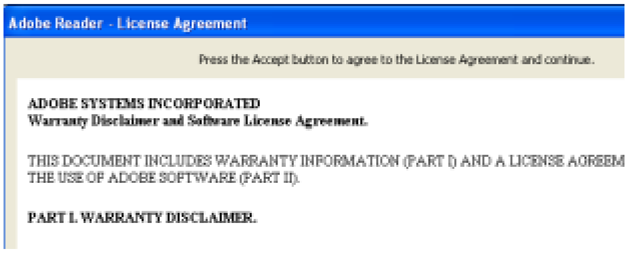
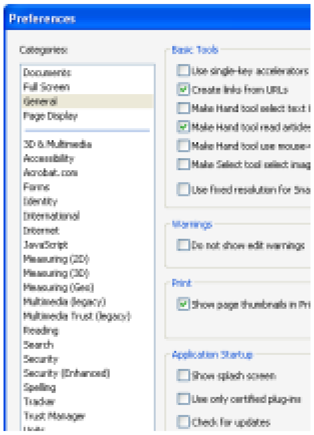
Step	Details
Step 56: To analyze PDF files, download Adobe Reader to the native host and copy it to the VM. This procedure uses Adobe Reader 9.0 as an example.	1 Install Adobe Reader 9.0 in the VM. 2 Open Adobe Reader and click **Accept**.  Adobe Reader - License Agreement Press the Accept button to agree to the License Agreement and continue. ADOBE SYSTEMS INCORPORATED Warranty Disclaimer and Software License Agreement. THIS DOCUMENT INCLUDES WARRANTY INFORMATION (PART I) AND A LICENSE AGREEM THE USE OF ADOBE SOFTWARE (PART II). PART I. WARRANTY DISCLAIMER. 3 a In Adobe Reader, select **Edit** | **Preferences** | **General** and deselect **Check for updates.** b In Adobe Reader, select **Help** | **Check for updates** | **Preferences** and deselect **Adobe Updates.**  Preferences Categories: Documents Full Screen General Page Display 3D & Multimedia Accessibility Acrobat.com Forms Identity International Internet JavaScript Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Reading Search Security Security (Enhanced) Spelling Tracker Trust Manager Basic Tools □ Use single-key accelerators ☑ Create links from URLs □ Make Hand tool select text ☑ Make Hand tool read articles □ Make Hand tool use mouse- □ Make Select tool select imag □ Use fixed resolution for Sna Warnings □ Do not show edit warnings Print ☑ Show page thumbnails in Pri Application Startup □ Show splash screen □ Use only certified plug-ins □ Check for updates
Step 57: Download the following on to the native host and then install them on the VM.	1 Download Microsoft Visual C++ 2005 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=3387and install it. 2 Download Microsoft Visual C++ 2008 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5582and install it. 3 Download Microsoft Visual C++ 2010 Redistributable Package (x86) from http://www.microsoft.com/en-us/download/details.aspx?id=5555and install it. 4 Download Microsoft .NET Framework 2.0 Service Pack 2 (x86 version) from http://www.microsoft.com/en-us/download/details.aspx?id=1639and install it.
Step 58: To analyze JAR files, download and install Java Runtime Environment.	1 Goto https://community.mcafee.com/docs/DOC-6858. 2 Refer **Java installation guidance.docx.**

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

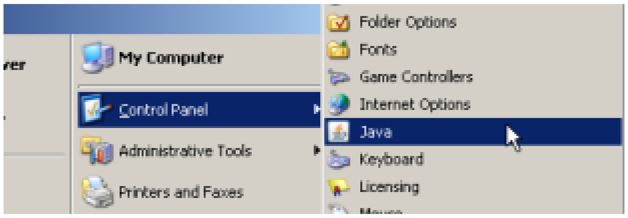
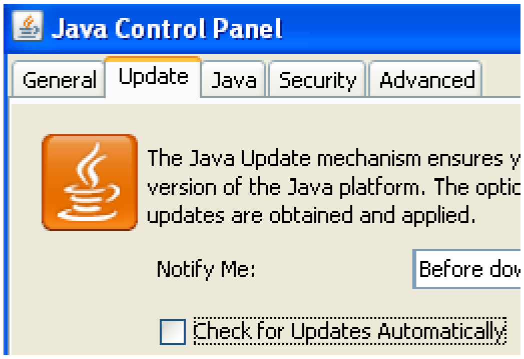
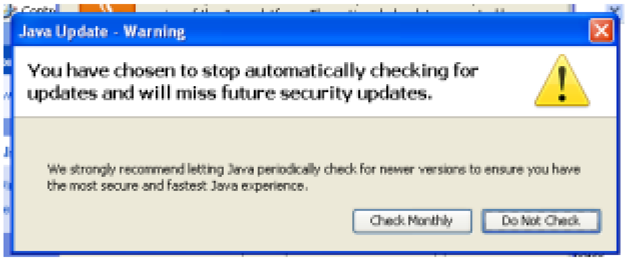
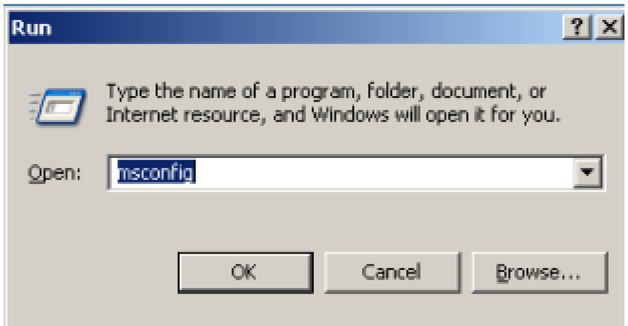
Step	Details
Step 59: Open Java in the Control Panel.	 My Computer Control Panel Administrative Tools Printers and Faxes Folder Options Fonts Game Controllers Internet Options Java Keyboard Licensing
Step 60: In the **Update** tab, deselect **Check for Updates Automatically.**	Java Control Panel The Java Update mechanism ensures y version of the Java platform. The optic updates are obtained and applied. Notify Me: Before dov □ Check for Updates Automatically
Step 61: In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel.	Java Update - Warning You have chosen to stop automatically checking for updates and will miss future security updates. We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.
Step 62: In the Windows Run dialog, enter `msconfig`.	Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: msconfig

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

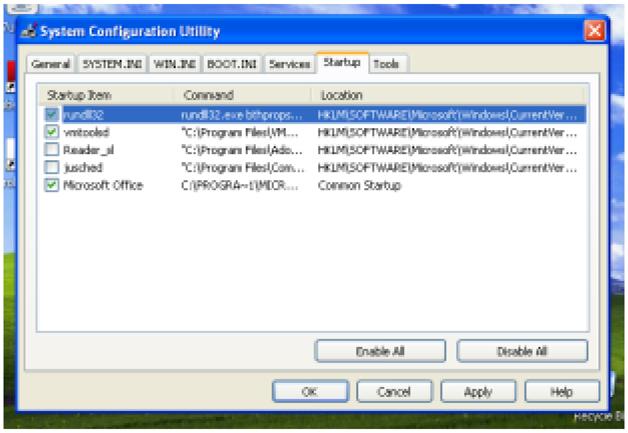
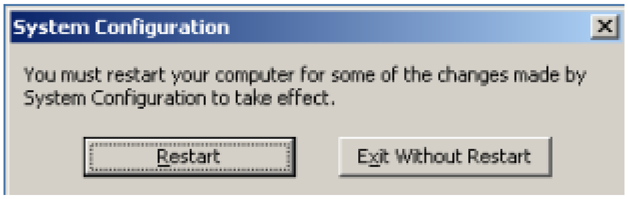
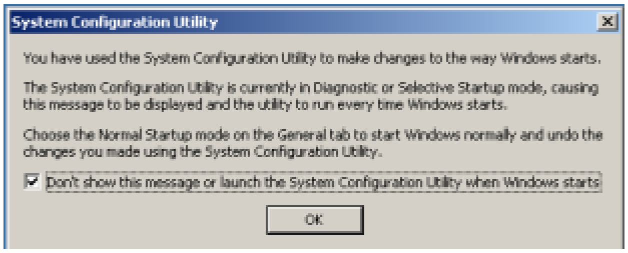
Step	Details
Step 63: In the System Configuration utility, go to the **Startup** tab.	 System Configuration Utility General · SYSTEM.INI · WIN.INI · BOOT.INI · Services · Startup · Tools Startup Item · Command · Location ☑ rundll32 · rundll32.exe bthprops... · HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☑ vmtoolsd · "C:\Program Files\VM... · HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☐ Reader_sl · "C:\Program Files\Ado... · HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☐ jusched · "C:\Program Files\Com... · HKLM\SOFTWARE\Microsoft\Windows\CurrentVer... ☑ Microsoft Office · C:\PROGRA~1\MICR... · Common Startup Enable All · Disable All OK · Cancel · Apply · Help Deselect *reader_sl* and *jusched* and then click **OK**. reader_sl is displayed only if you have installed Adobe Reader.
Step 64: In the **System Configuration** dialog, click **Restart**.	 System Configuration You must restart your computer for some of the changes made by System Configuration to take effect. Restart · Exit Without Restart
Step 65: In the **System Configuration Utility** dialog, select **Don't show this message or launch the System Configuration Utility when Windows starts** and click **OK**.	 System Configuration Utility You have used the System Configuration Utility to make changes to the way Windows starts. The System Configuration Utility is currently in Diagnostic or Selective Startup mode, causing this message to be displayed and the utility to run every time Windows starts. Choose the Normal Startup mode on the General tab to start Windows normally and undo the changes you made using the System Configuration Utility. ☑ Don't show this message or launch the System Configuration Utility when Windows starts OK

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

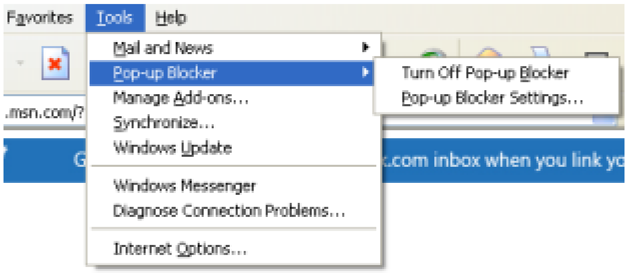
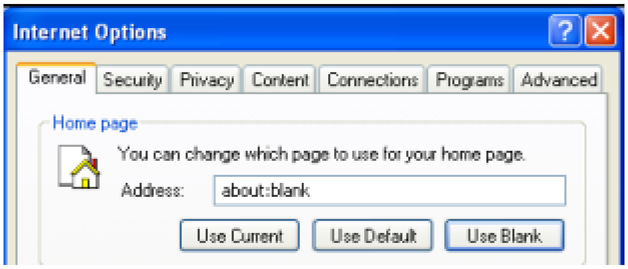
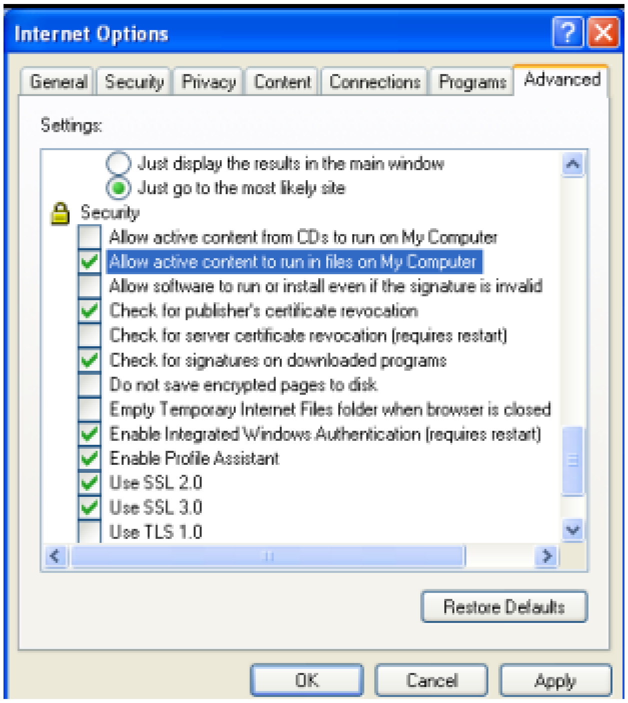
Step	Details
Step 66: Open the default browser and set it up for malware analysis. This procedure uses Internet Explorer as an example.	1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** | **Pop-up Blocker** | **Turn on Pop-up Blocker.**  Favorites Tools Help Mail and News Pop-up Blocker Manage Add-ons... Synchronize... Windows Update Windows Messenger Diagnose Connection Problems... Internet Options... Turn Off Pop-up Blocker Pop-up Blocker Settings... .msn.com/? .com inbox when you link yo 2 Select **Tools** | **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.  Internet Options General Security Privacy Content Connections Programs Advanced Home page Use Current Use Default Use Blank You can change which page to use for your home page. Address: about:blank 3 Go to the **Advanced** tab of the Internet Options and locate **Security.** 4 Select **Allow active content to run in files on My Computer.**

Table 5-3 Create a VMDK file from Windows 2003 Server SP1 or SP2 ISO image *(continued)*

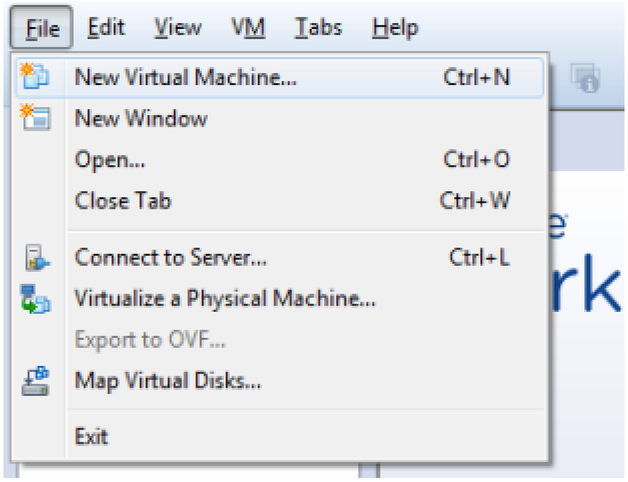
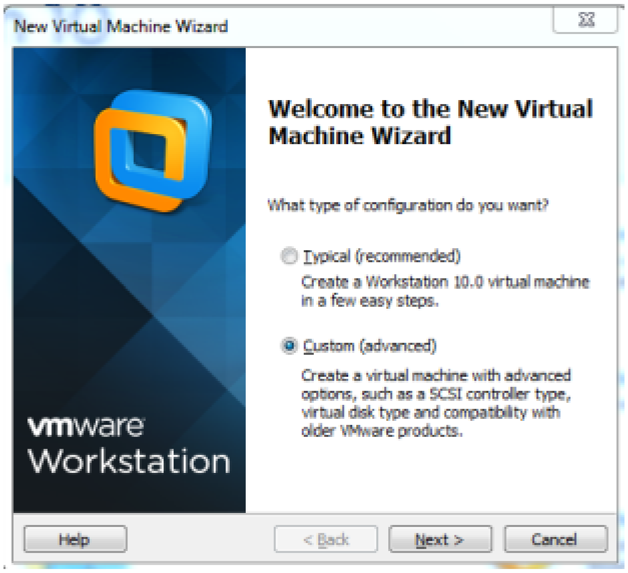
Step	Details
	 Internet Options General Security Privacy Content Connections Programs Advanced Settings: Restore Defaults OK Cancel Apply ○ Just display the results in the main window ● Just go to the most likely site Security □ Allow active content from CDs to run on My Computer ☑ Allow active content to run in files on My Computer □ Allow software to run or install even if the signature is invalid ☑ Check for publisher's certificate revocation □ Check for server certificate revocation (requires restart) ☑ Check for signatures on downloaded programs □ Do not save encrypted pages to disk □ Empty Temporary Internet Files folder when browser is closed ☑ Enable Integrated Windows Authentication (requires restart) ☑ Enable Profile Assistant ☑ Use SSL 2.0 ☑ Use SSL 3.0 □ Use TLS 1.0 5 Click **OK**.
Step 67: To dynamically analyze Flash files (SWF), download the required version of Adobe Flash.	1 Goto https://community.mcafee.com/docs/DOC-6859. 2 Refer **Adobe flash player installation guidance.docx**.
Step 68: Shut down virtualMachineImage by selecting **Start** | **Shut down** | **Shut down** | **OK**.	
Step 69: Go to the location that you provided in step 7 to find the VMDK file named as `virtualMachineImage-flat.vmdk`	

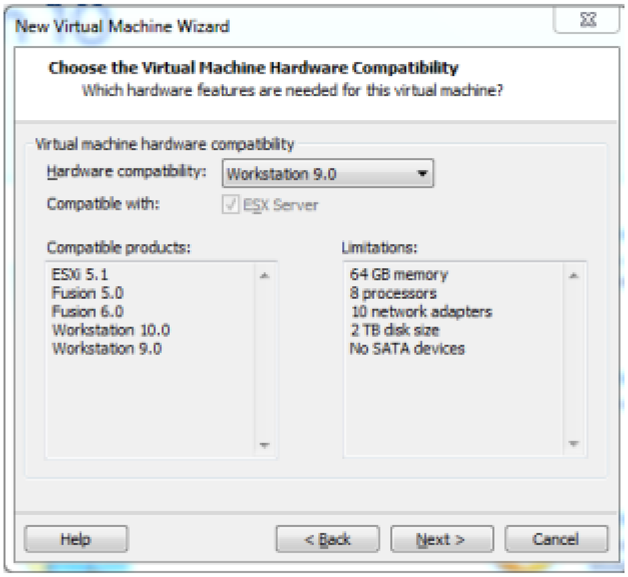
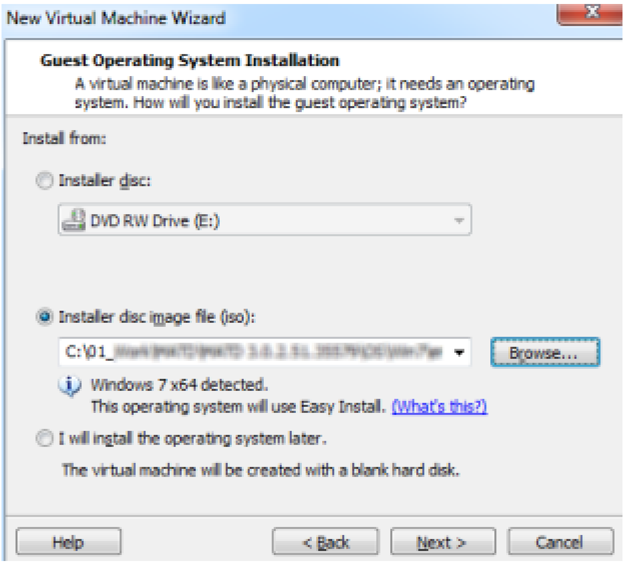
Create a VMDK file for Windows 7

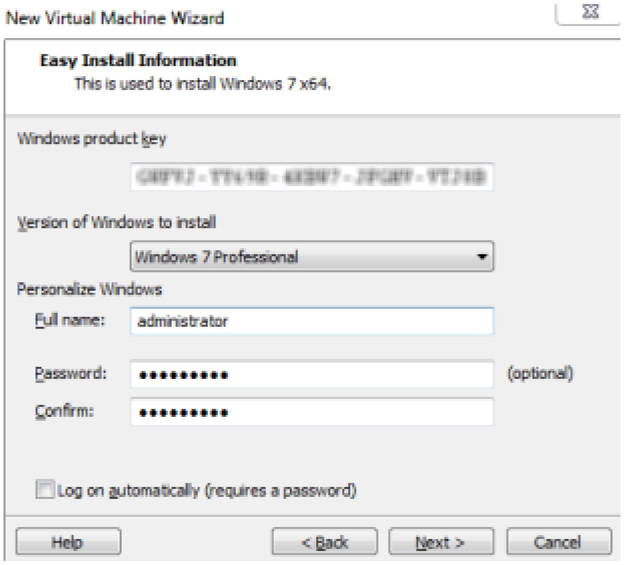
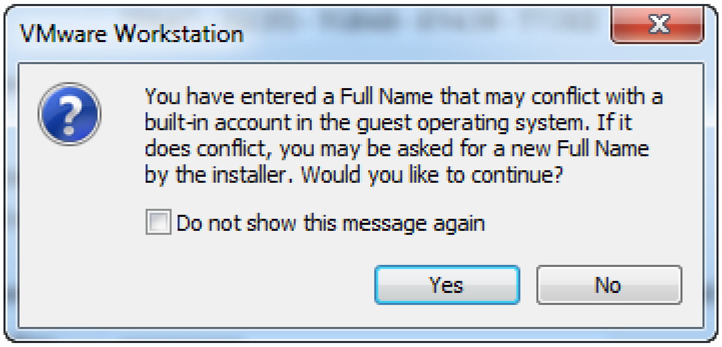
Before you begin

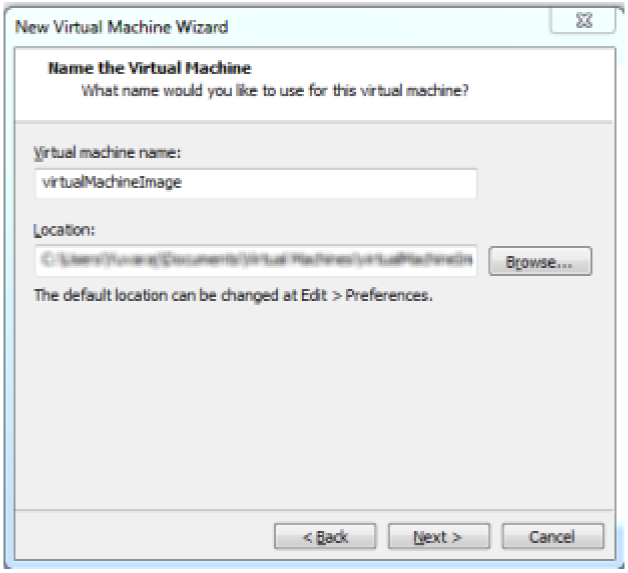
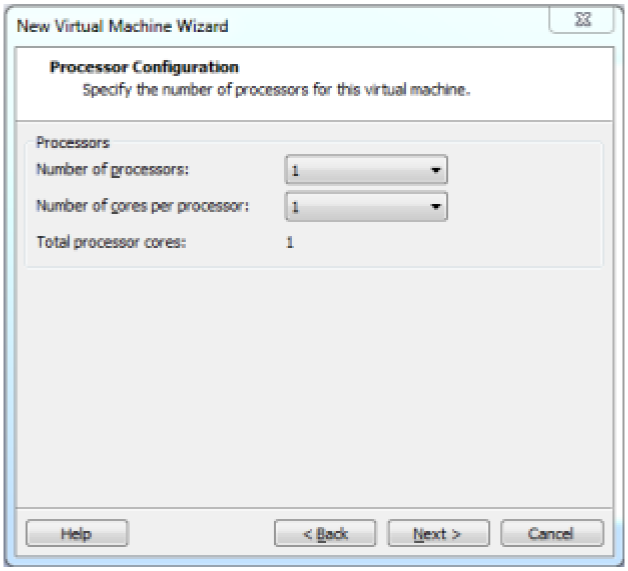
- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure that you have the ISO image of Windows 7 SP1 32 or 64 bit for which you need to create the VMDK file. Windows Enterprise edition and Windows Professional are supported.
- Make sure you have the license key for the operating system.

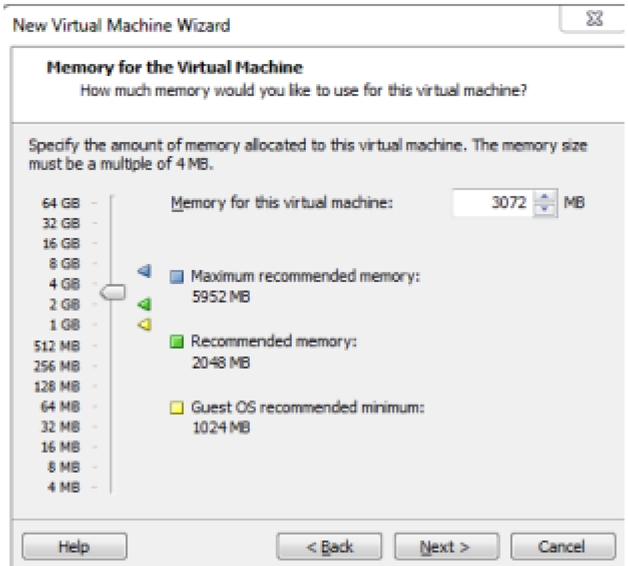
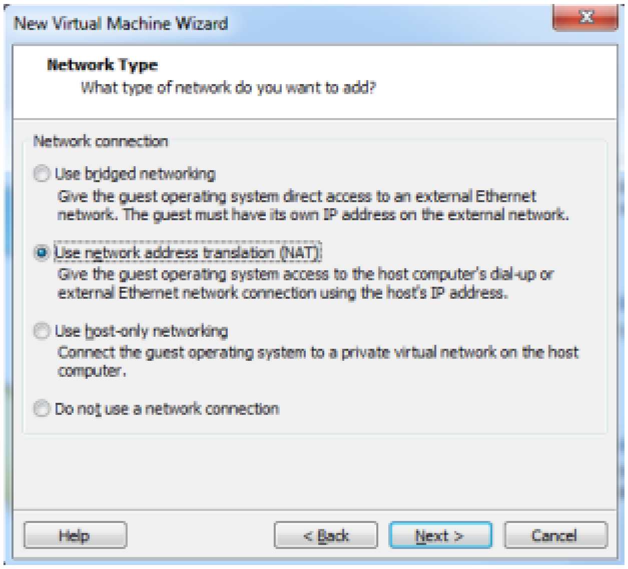
Use this procedure to create VMDK files from an ISO image of Windows 7 SP1 32 or 64 bit.

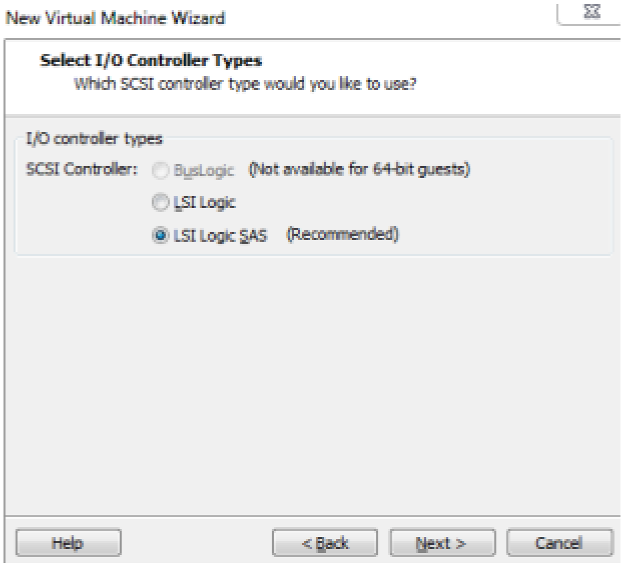
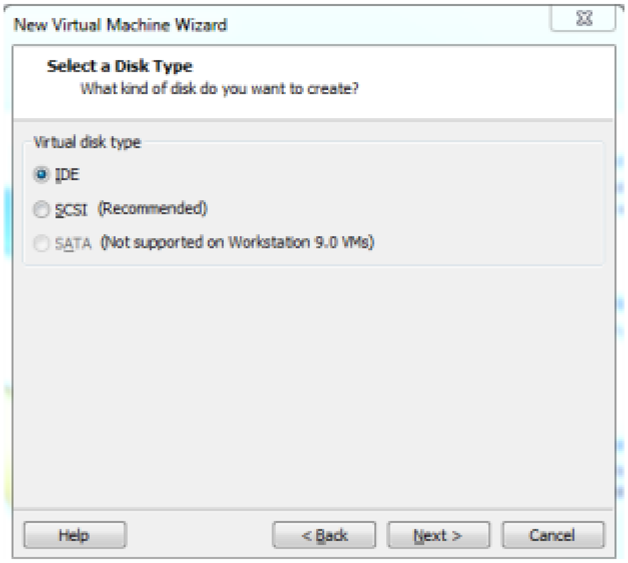
Step	Details
Step 1: Start the VMware Workstation.	This procedure uses VMware Workstation 10 as an example.
Step 2: In the VMware Workstation page, select **File | New Virtual Machine.**	 File Edit View VM Tabs Help New Virtual Machine... Ctrl+N New Window Open... Ctrl+O Close Tab Ctrl+W Connect to Server... Ctrl+L Virtualize a Physical Machine... Export to OVF... Map Virtual Disks... Exit
Step 3: In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.**	 New Virtual Machine Wizard **Welcome to the New Virtual Machine Wizard** What type of configuration do you want? ○ Typical (recommended) Create a Workstation 10.0 virtual machine in a few easy steps. ● Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatbility with older VMware products.

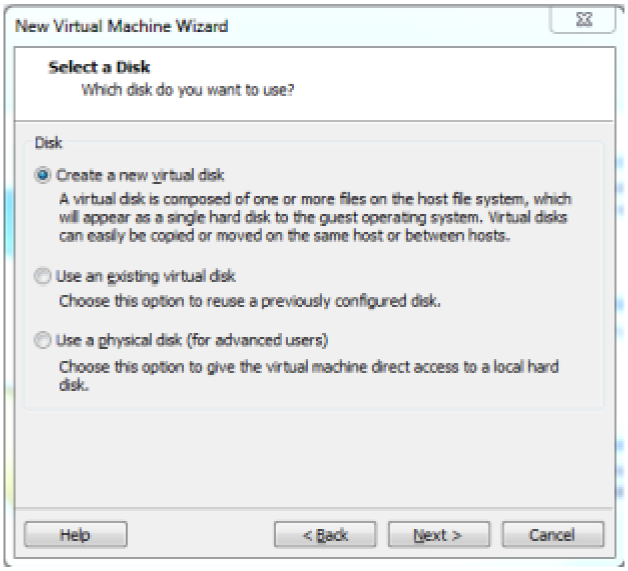
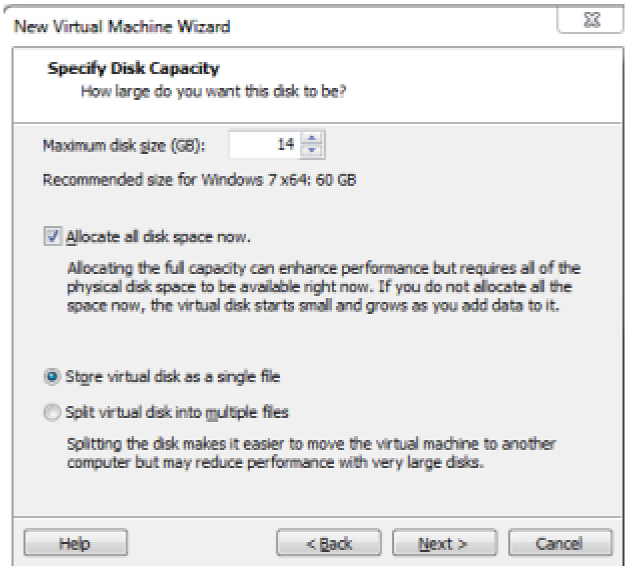
Step	Details
Step 4: In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next.**	 New Virtual Machine Wizard **Choose the Virtual Machine Hardware Compatibility** Which hardware features are needed for this virtual machine? Virtual machine hardware compatibility Hardware compatibility: Workstation 9.0 Compatible with: ☑ ESX Server Compatible products: ESXi 5.1, Fusion 5.0, Fusion 6.0, Workstation 10.0, Workstation 9.0 Limitations: 64 GB memory, 8 processors, 10 network adapters, 2 TB disk size, No SATA devices
Step 5: In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next.**	 New Virtual Machine Wizard **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: ○ Installer disc: DVD RW Drive (E:) ● Installer disc image file (iso): C:\01_[redacted] Windows 7 x64 detected. This operating system will use Easy Install. (What's this?) ○ I will install the operating system later. The virtual machine will be created with a blank hard disk.

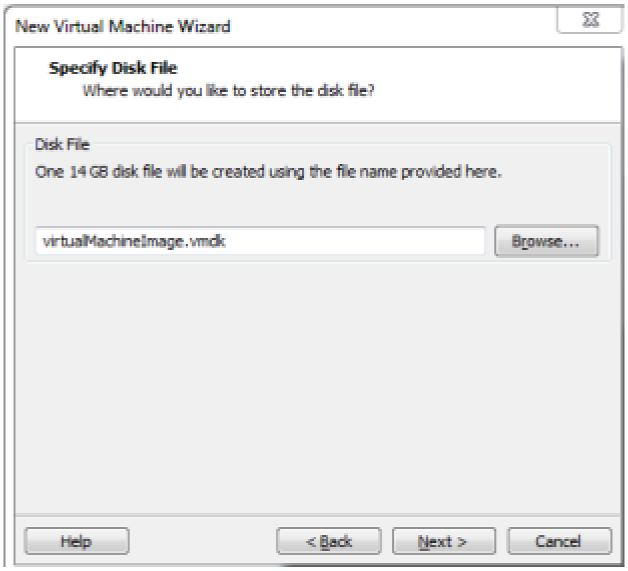
Step	Details
Step 6: Enter the information in the **Easy Install Information** window and then click **Next**.	• **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file. • **Full name** — You must enter `administrator` as the **Full name.** • **Password** — You must enter `cr@cker42` as the password. This is the password that Advanced Threat Defense uses to log on to the VM. • **Confirm** — Enter `cr@cker42` again to confirm. • **Log on automatically (requires a password)** — Deselect this box.  New Virtual Machine Wizard **Easy Install Information** This is used to install Windows 7 x64. Windows product key [illegible] Version of Windows to install Windows 7 Professional Personalize Windows Full name: administrator Password: ••••••••• (optional) Confirm: ••••••••• ☐ Log on automatically (requires a password) Help < Back Next > Cancel
Step 7: If the **VMware Workstation** message displays, click **Yes**.	 VMware Workstation You have entered a Full Name that may conflict with a built-in account in the guest operating system. If it does conflict, you may be asked for a new Full Name by the installer. Would you like to continue? ☐ Do not show this message again Yes No

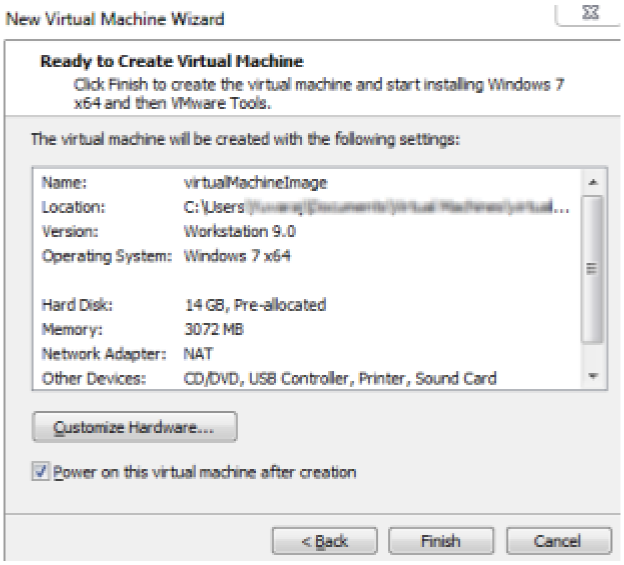
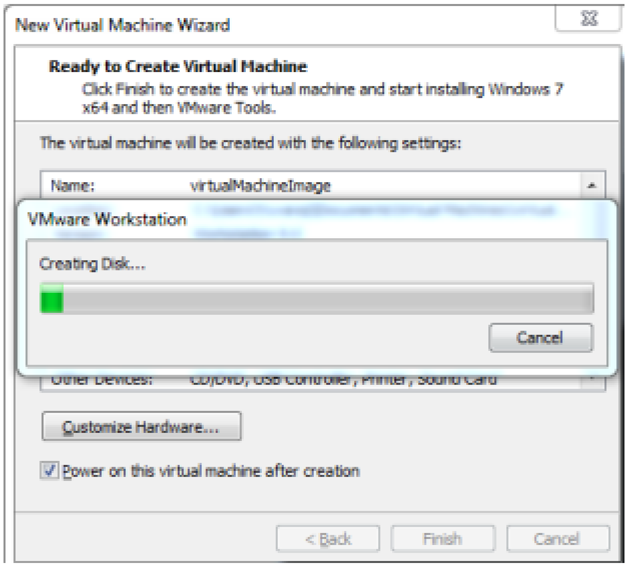
Step	Details
Step 8: Enter the information in the **Name the Virtual Machine** window and then click **Next**.	• **Virtual Machine name** — You must enter `virtualMachineImage` as the name. • **Location** — Browse and select the folder where you want to create the VMDK file.  New Virtual Machine Wizard **Name the Virtual Machine** What name would you like to use for this virtual machine? Virtual machine name: virtualMachineImage Location: [redacted] The default location can be changed at Edit > Preferences.
Step 9: In the **Processor Configuration** window, leave the default values and click **Next**.	 New Virtual Machine Wizard **Processor Configuration** Specify the number of processors for this virtual machine. Processors Number of processors: 1 Number of cores per processor: 1 Total processor cores: 1

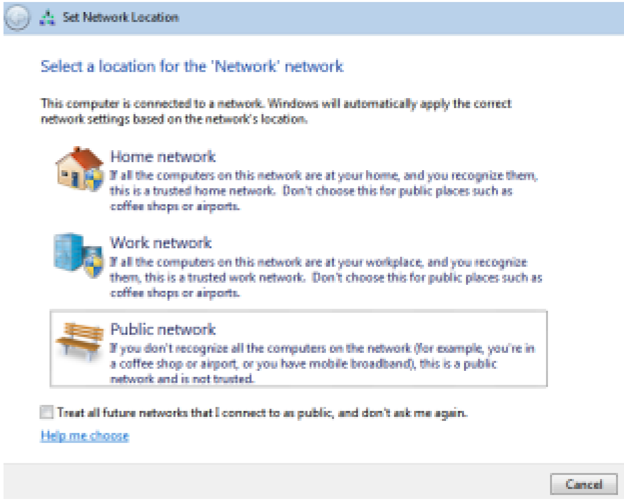
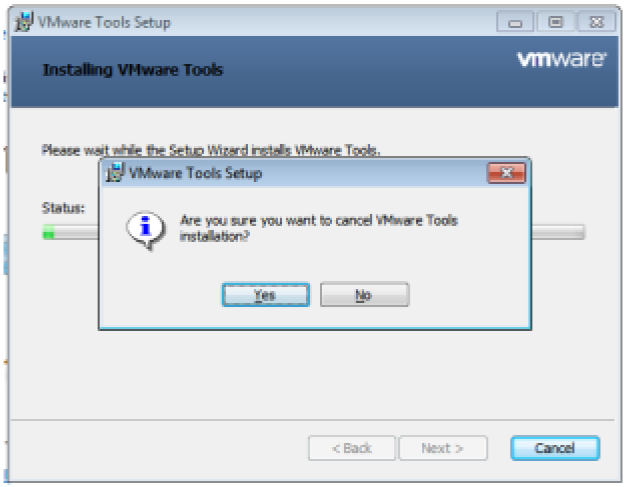
Step	Details
Step 10: In the **Memory for the Virtual Machine** window, set 3072 MB as the memory.	 New Virtual Machine Wizard **Memory for the Virtual Machine** How much memory would you like to use for this virtual machine? Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB. Memory for this virtual machine: 3072 MB Maximum recommended memory: 5952 MB Recommended memory: 2048 MB Guest OS recommended minimum: 1024 MB 64 GB 32 GB 16 GB 8 GB 4 GB 2 GB 1 GB 512 MB 256 MB 128 MB 64 MB 32 MB 16 MB 8 MB 4 MB Help < Back Next > Cancel
Step 11: In the **Network Type** window, leave the default selection.	 New Virtual Machine Wizard **Network Type** What type of network do you want to add? Network connection ○ Use bridged networking Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network. ● Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address. ○ Use host-only networking Connect the guest operating system to a private virtual network on the host computer. ○ Do not use a network connection

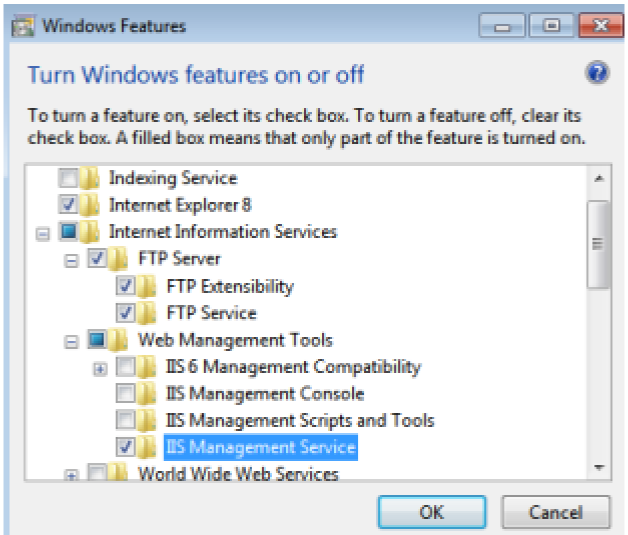
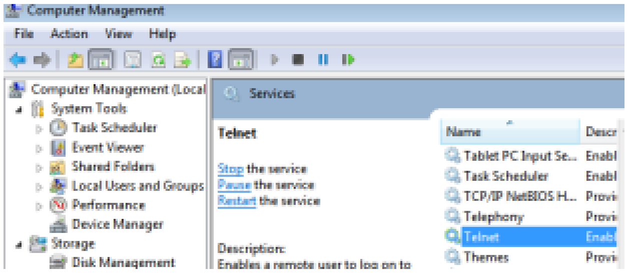
Step	Details
Step 12: In the **Select I/O Controller Types** , leave the default selection.	 New Virtual Machine Wizard **Select I/O Controller Types** Which SCSI controller type would you like to use? I/O controller types SCSI Controller: ○ BusLogic (Not available for 64-bit guests) ○ LSI Logic ● LSI Logic SAS (Recommended)
Step 13: In the **Select a Disk Type** page, select **IDE** and click **Next.** SCSI disks are not compatible with McAfee Advanced Threat Defense.	 New Virtual Machine Wizard **Select a Disk Type** What kind of disk do you want to create? Virtual disk type ● IDE ○ SCSI (Recommended) ○ SATA (Not supported on Workstation 9.0 VMs)

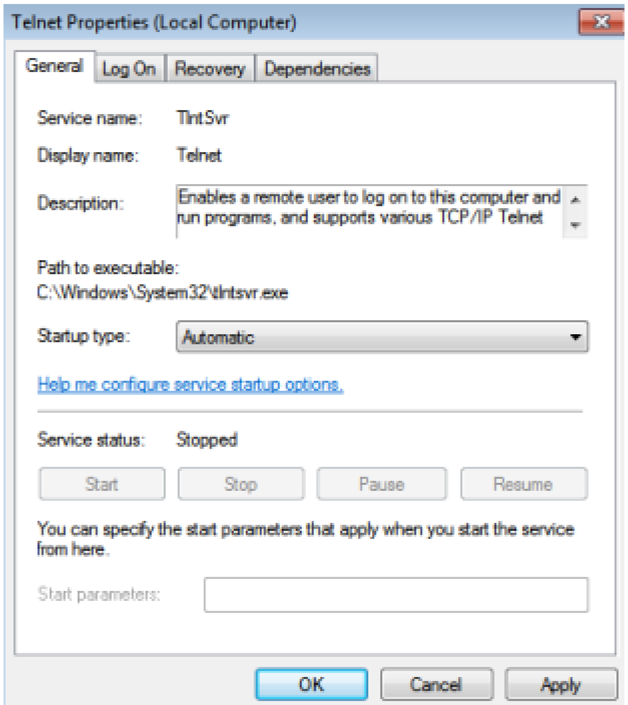
Step	Details
Step 14: In the **Select a Disk** window, select **Create a new virtual disk** and click **Next.**	 New Virtual Machine Wizard **Select a Disk** Which disk do you want to use? Disk ● Create a new virtual disk A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts. ○ Use an existing virtual disk Choose this option to reuse a previously configured disk. ○ Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard disk.
Step 15: Specify the details in the **Specify Disk Capacity** window and then click **Next**.	- **Maximum disk size (GB)** — For Windows 7, the maximum disk size can be 30 GB. However, for optimal performance, you must enter 14 GB and 12 GB for Windows 7 64-bit and Windows 7 32-bit, respectively. - Select **Allocate all disk space now.** - Select **Store virtual disk as a single file.**  New Virtual Machine Wizard **Specify Disk Capacity** How large do you want this disk to be? Maximum disk size (GB): 14 Recommended size for Windows 7 x64: 60 GB ☑ Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it. ● Store virtual disk as a single file ○ Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Step	Details
Step 16: In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next.** If you specified a different name for **Virtual Machine name**, that name is displayed here.	 New Virtual Machine Wizard **Specify Disk File** Where would you like to store the disk file? Disk File One 14 GB disk file will be created using the file name provided here. virtualMachineImage.vmdk

Step	Details
Step 17: Complete the following in the **Ready to Create Virtual Machine** window.	- **Power on this virtual machine after creation** — Select this option. - Click **Finish.** This step might take around 30 minutes to complete.  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows 7 x64 and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage Location: C:\Users\[redacted]... Version: Workstation 9.0 Operating System: Windows 7 x64 Hard Disk: 14 GB, Pre-allocated Memory: 3072 MB Network Adapter: NAT Other Devices: CD/DVD, USB Controller, Printer, Sound Card ☑ Power on this virtual machine after creation  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows 7 x64 and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage VMware Workstation Creating Disk... Other Devices: CD/DVD, USB Controller, Printer, Sound Card ☑ Power on this virtual machine after creation Cancel Customize Hardware... < Back Finish Cancel
Step 18: If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK.**	Windows begins to install, which might take around 15 minutes.

Step	Details
Step 19: If the **Set Network Location** window is displayed, select **Public Network** and select **Close.**	 Set Network Location Select a location for the 'Network' network This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location. Home network If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports. Work network If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports. Public network If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted. □ Treat all future networks that I connect to as public, and don't ask me again.
Step 20: Stop the VMware Tools installation. The VMware Tools are not compatible with Advanced Threat Defense. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready.	 VMware Tools Setup Installing VMware Tools Please wait while the Setup Wizard installs VMware Tools. Status: VMware Tools Setup Are you sure you want to cancel VMware Tools installation?
Step 23: In the VM, turn off the Windows Firewall.	1 Select **Start** | **Control Panel** | **System and Security** | **Windows Firewall** | **Turn on Windows Firewall On or Off** 2 Select **Turn off Windows Firewall (not recommended)** for both **Home or work(private) network location settings** and **Public network location settings** and then click **OK.**

Step	Details
Step 24: Select **Start** | **Control Panel** | **Programs** | **Programs and Features** | **Turn Windows feature on or off** and complete the following.	1 Select **Internet Information Services** | **FTP server** and select **FTP Extensibility**. 2 Select **Internet Information Services** | **Web Management Tools** and select **IIS Management Service**. 3 Select **Telnet Server** and press OK. This operation might take around 5 minutes to complete.  Windows Features Turn Windows features on or off To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on. □ Indexing Service ☑ Internet Explorer 8 ■ Internet Information Services ☑ FTP Server ☑ FTP Extensibility ☑ FTP Service ■ Web Management Tools □ IIS 6 Management Compatibility □ IIS Management Console □ IIS Management Scripts and Tools ☑ IIS Management Service □ World Wide Web Services OK Cancel
Step 25: Click **Start** and right-click **Computer**. Then select **Manage** | **Services and Applications** | **Services**. Then double-click **Telnet**.	 Computer Management File Action View Help Computer Management (Local System Tools Task Scheduler Event Viewer Shared Folders Local Users and Groups Performance Device Manager Storage Disk Management Services Telnet Stop the service Pause the service Restart the service Description: Enables a remote user to log on to Name Descr Tablet PC Input Se... Enabl Task Scheduler Enabl TCP/IP NetBIOS H... Provi Telephony Provi Telnet Enabl Themes Provi

Step	Details
Step 26: In the Telnet Properties (Local Computer) dialog, select **Automatic** from the **Startup type** list. Then select **Apply** | **Start** | **OK**.	 Telnet Properties (Local Computer) Service name: TlntSvr Display name: Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet Path to executable: C:\Windows\System32\tlntsvr.exe Startup type: Automatic Help me configure service startup options. Service status: Stopped You can specify the start parameters that apply when you start the service from here. Start parameters: General Log On Recovery Dependencies Start Stop Pause Resume OK Cancel Apply

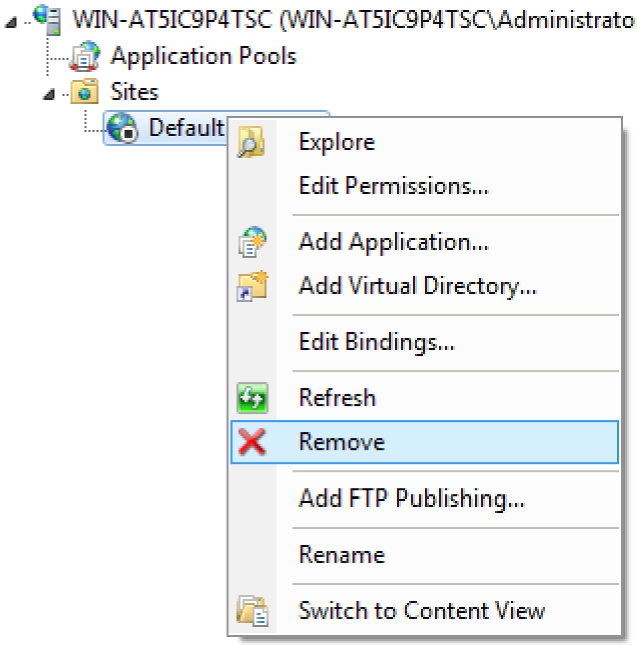
<table>
<tr><th>Step</th><th>Details</th></tr>
<tr><td>

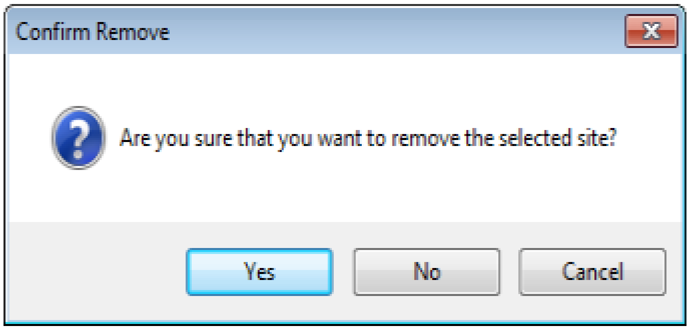
Step 27: Enable FTP on the VM.

In the virtualMachineImage, select **Start** | **Control Panel** | **System and Security** | **Administrative Tools**. Double-click **Internet Information Services(IIS) Manager**, expand the tree under **Hostname**, and complete the following:

</td><td>

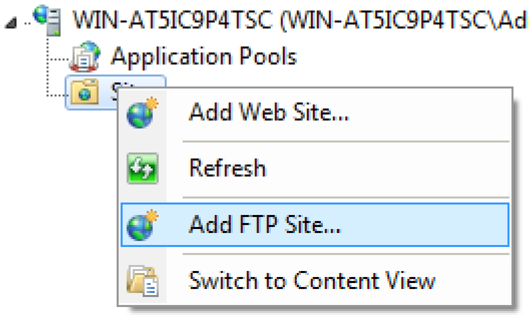
1 Select **Sites** and right-click **Default Web Site** and remove. Confirm by clicking **Yes**.





Are you sure that you want to remove the selected site?

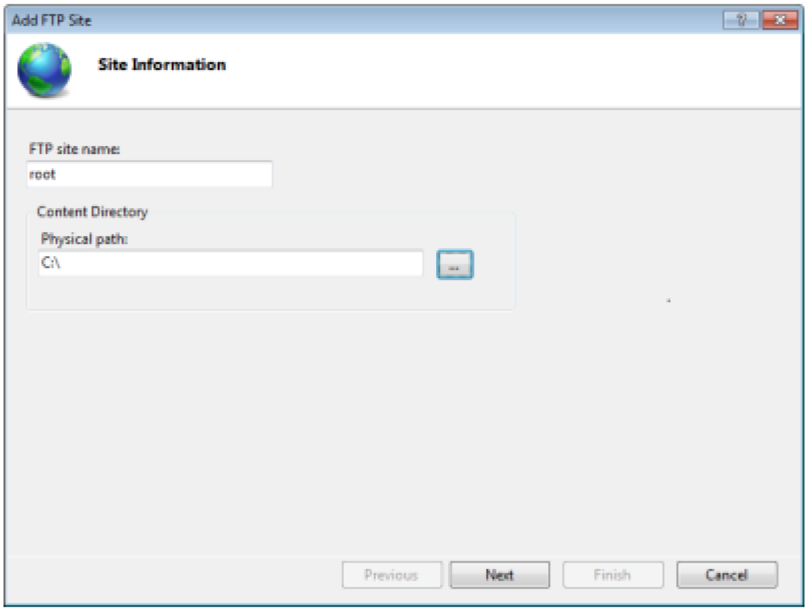
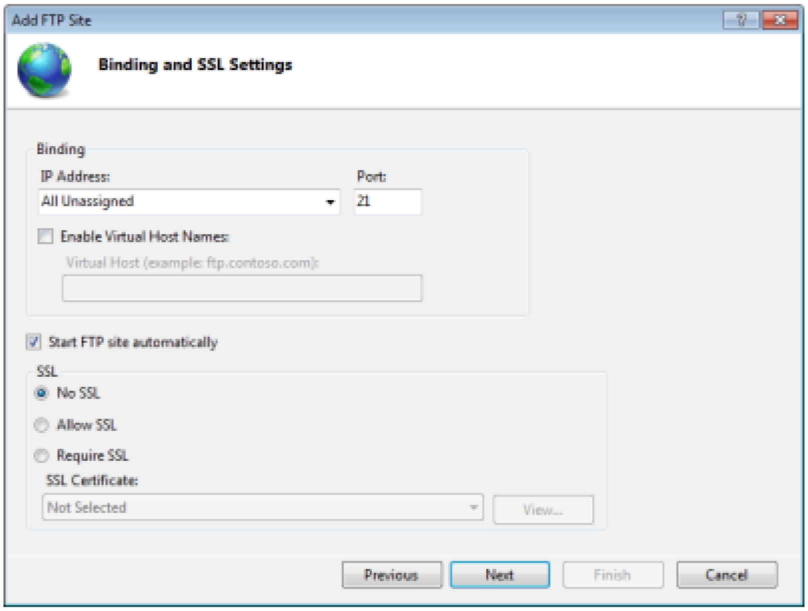
2 Right-click **Sites** and select **Add FTP Site**. Then complete the following.

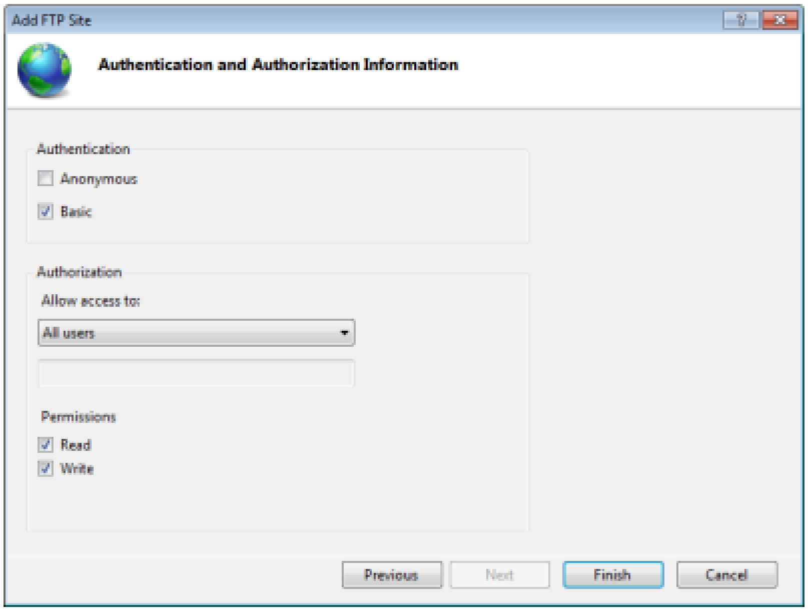
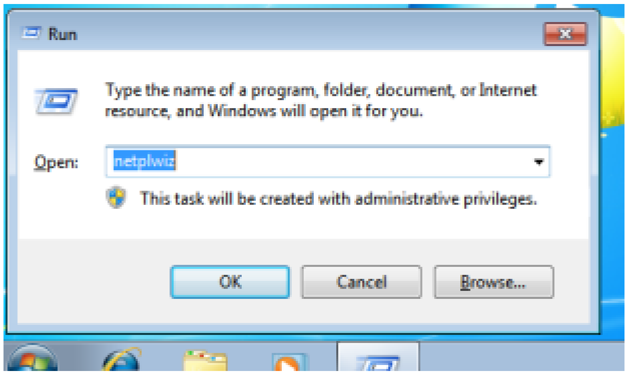


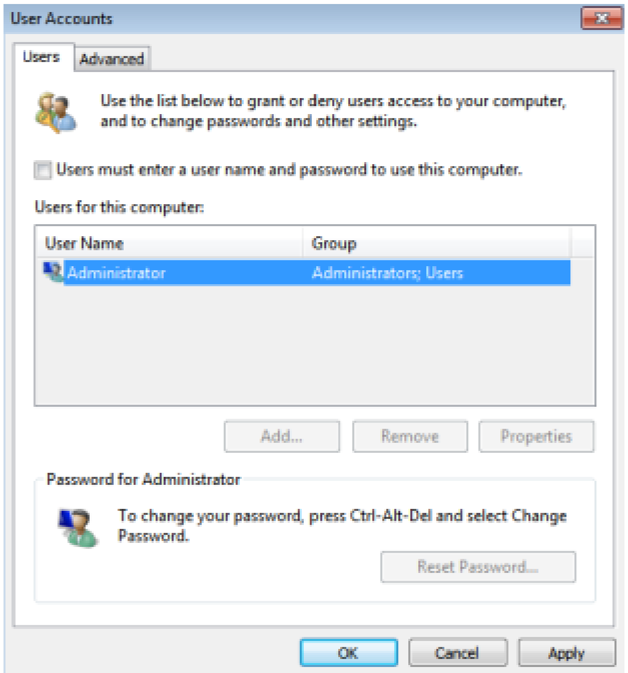
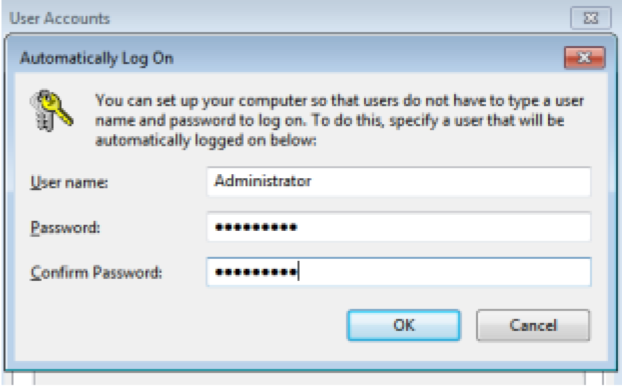
a For **FTP site name**, enter `root`.

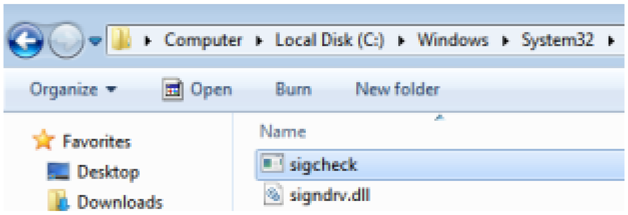
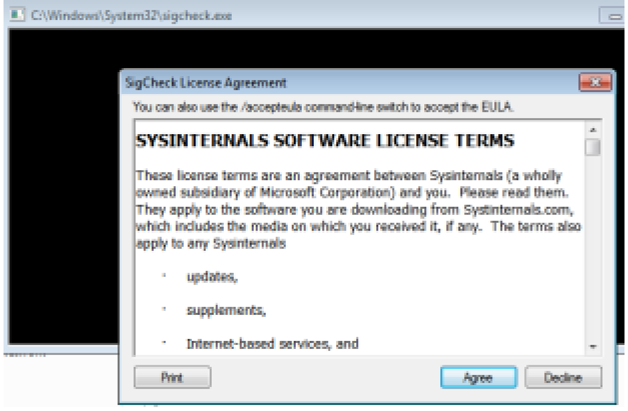
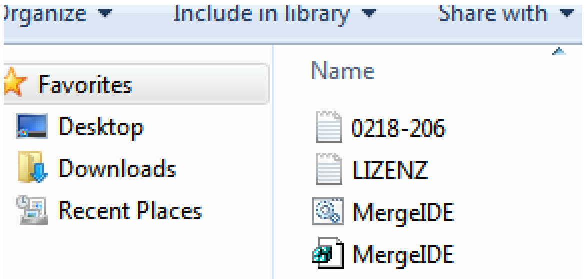
b **Physical Path: C:\.**

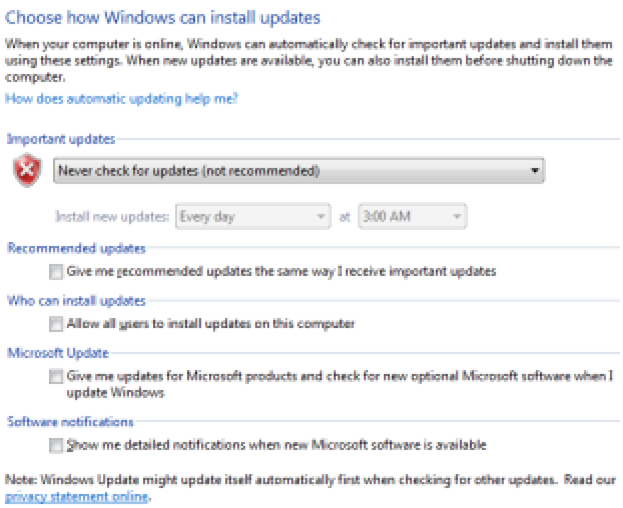
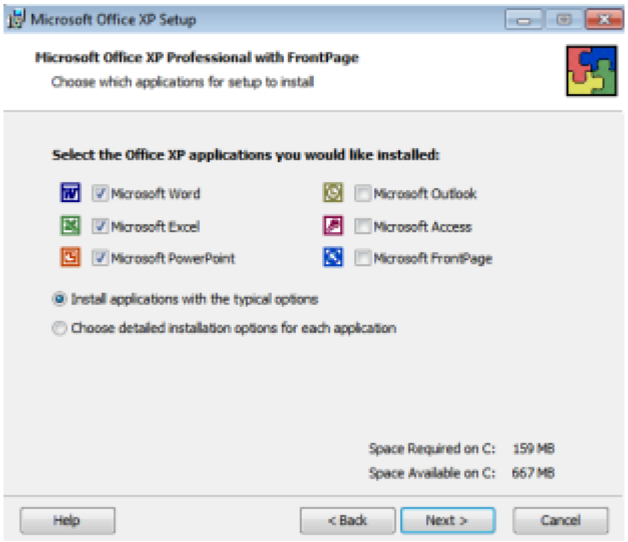
</td></tr>
</table>

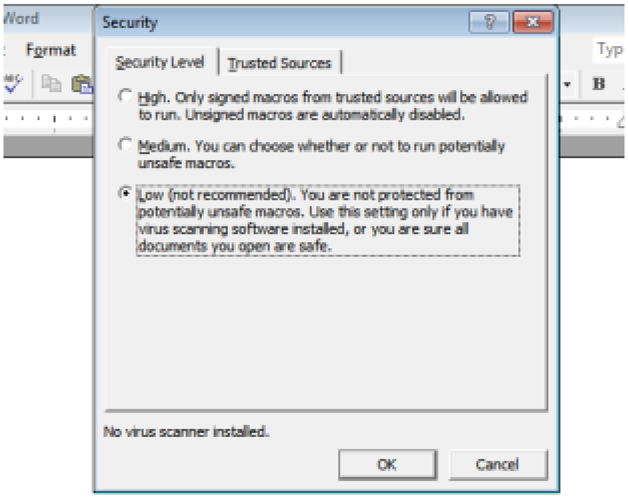
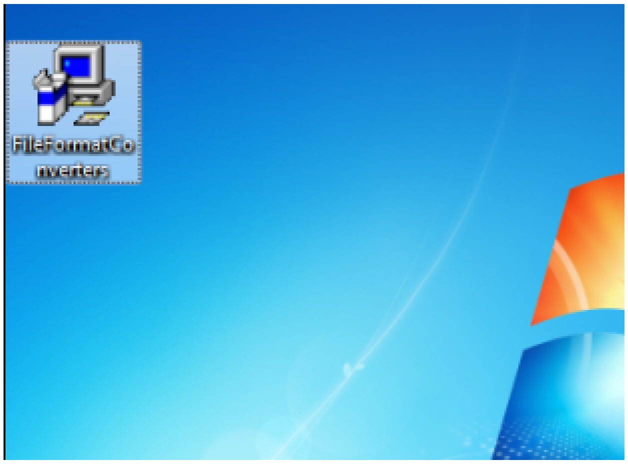
Step	Details
	c Click **Next**.  **Site Information** FTP site name: root Content Directory Physical path: C:\ ... **3** For **Bindings and SSL Settings**, select **No SSL**. For all other fields, leave the default values and click **Next**.  Add FTP Site Previous Next Finish Cancel View... **Binding and SSL Settings** Binding IP Address: All Unassigned Port: 21 □ Enable Virtual Host Names: Virtual Host (example: ftp.contoso.com): ☑ Start FTP site automatically SSL ● No SSL ○ Allow SSL ○ Require SSL SSL Certificate: Not Selected **Figure 5-1 Binding and SSL settings** **4** For **Authentication and Authorization Information** complete the following. **a** Select **Basic**. **b** For **Allow access to**, select **All Users**. **c** For **Permissions**, select both **Read** and **Write**, and then click **Finish**.

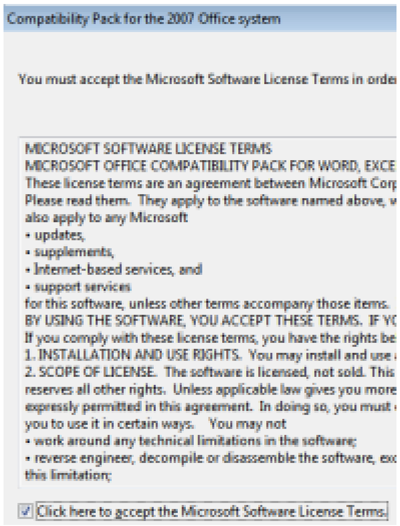
Step	Details
	d Close the **Internet Information Services (IIS) Manager**.  Add FTP Site **Authentication and Authorization Information** Authentication ☐ Anonymous ☑ Basic Authorization Allow access to: All users Permissions ☑ Read ☑ Write
Step 28: select **Start** | **Run**, enter `netplwiz` and press **OK**.	 Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: netplwiz This task will be created with administrative privileges.

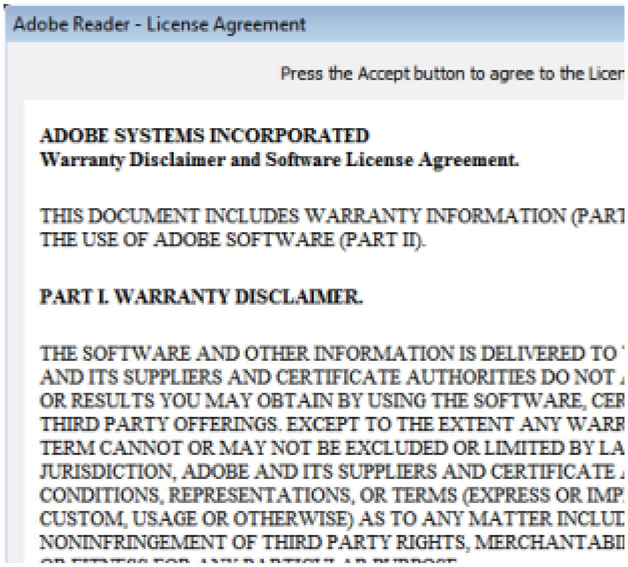
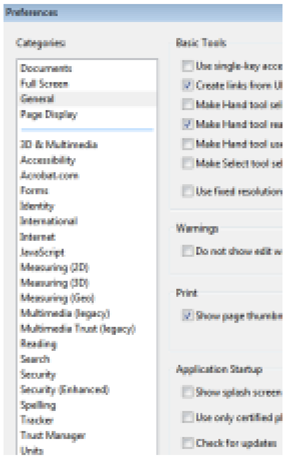
Step	Details
Step 29: In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply.**	 User Accounts Users Advanced Use the list below to grant or deny users access to your computer, and to change passwords and other settings. ☐ Users must enter a user name and password to use this computer. Users for this computer: User Name Group Administrator Administrators; Users Add... Remove Properties Password for Administrator To change your password, press Ctrl-Alt-Del and select Change Password. Reset Password... OK Cancel Apply
Step 30: In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes.	• **User name** — Enter `Administrator` • **Password** — Enter `cr@cker42` • **Confirm Password** — Enter `cr@cker42`  You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below: User name: Administrator Password: ••••••••• Confirm Password: •••••••••
Step 31: Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx.	The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation.
Step 32: Extract sigcheck.zip to `C:\WINDOWS\system32` location.	

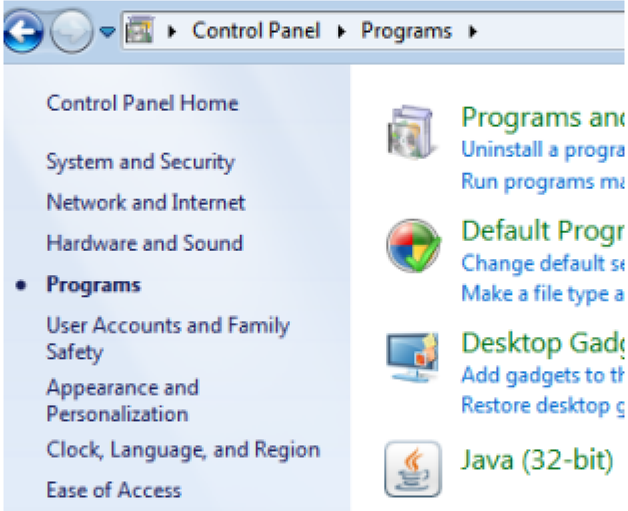
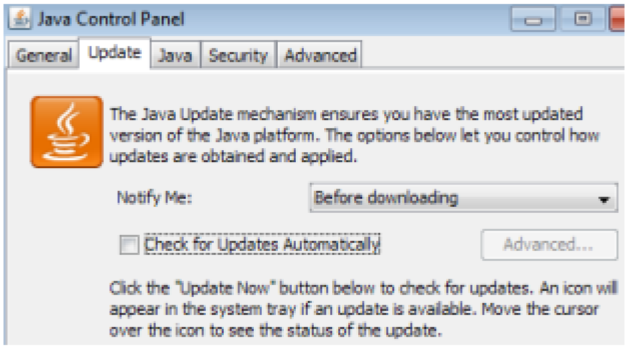
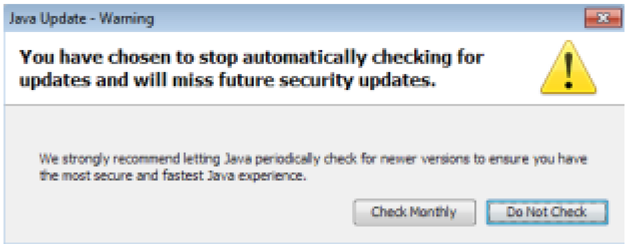
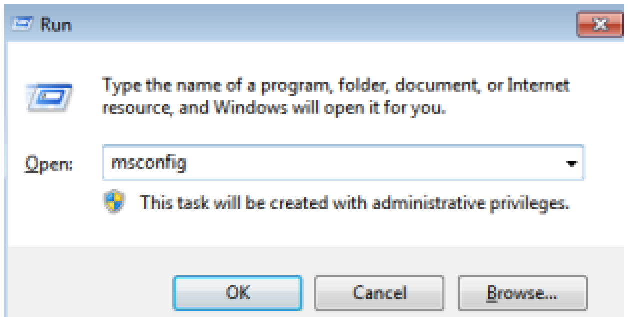
Step	Details
Step 33: In Windows Explorer, go to C:\WINDOWS\system32 and double-click **sigcheck.exe**.	 Computer ▸ Local Disk (C:) ▸ Windows ▸ System32 ▸ Organize ▾ Open Burn New folder Favorites Desktop Downloads Name sigcheck signdrv.dll
Step 34 Click **Agree** for **Sigcheck License Agreement**. After you click on **Agree**, no confirmation message is displayed.	 C:\Windows\System32\sigcheck.exe SigCheck License Agreement You can also use the /accepteula command-line switch to accept the EULA. **SYSINTERNALS SOFTWARE LICENSE TERMS** These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals · updates, · supplements, · Internet-based services, and
Step 35: Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM.	 Organize ▾ Include in library ▾ Share with ▾ Favorites Desktop Downloads Recent Places Name 0218-206 LIZENZ MergeIDE MergeIDE
Step 36: Extract MergeIDE.zip and run the MergeIDE batch file in the VM.	• If prompted, select **Run** in the warning message. • Close Windows Explorer.

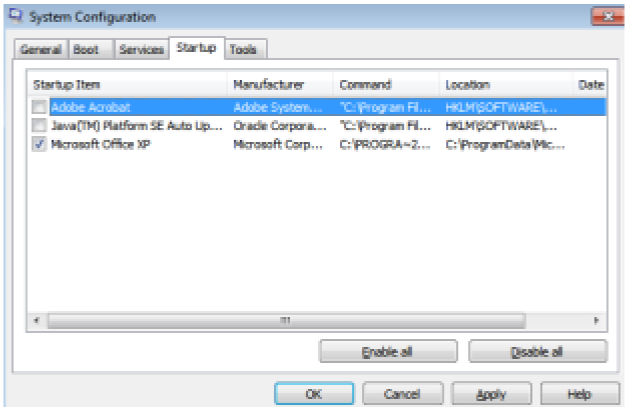
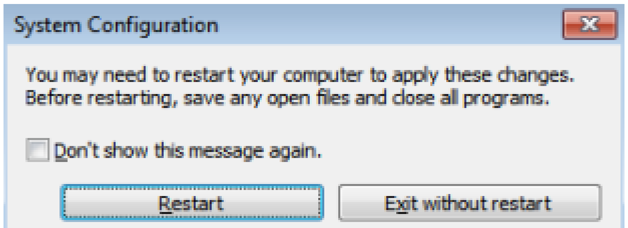
Step	Details
Step 37: Disable Windows updates.	1 Select **Start** | **Control Panel** | **Windows Update** | **Change settings.** 2 In the **Change settings** page, complete the following. a In the **Important updates** select **Never check for updates (not recommended).** b Deselect the check boxes under **Recommended updates, Who can install updates, Microsoft update, Software notifications.**  Choose how Windows can install updates When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer. How does automatic updating help me? Important updates Never check for updates (not recommended) Install new updates: Every day at 3:00 AM Recommended updates □ Give me recommended updates the same way I receive important updates Who can install updates □ Allow all users to install updates on this computer Microsoft Update □ Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows Software notifications □ Show me detailed notifications when new Microsoft software is available Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online. 3 Click **OK.**
Step 38: To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine.	 Microsoft Office XP Setup Microsoft Office XP Professional with FrontPage Choose which applications for setup to install Select the Office XP applications you would like installed: ☑ Microsoft Word □ Microsoft Outlook ☑ Microsoft Excel □ Microsoft Access ☑ Microsoft PowerPoint □ Microsoft FrontPage ● Install applications with the typical options ○ Choose detailed installation options for each application Space Required on C: 159 MB Space Available on C: 667 MB

Step	Details
Step 39: Lower the security to run macros for the Office applications.	• Open Microsoft Word 2003 and select **Tools** | **Macro** | **Security** and then select **Low** and click **OK**.  Security Security Level | Trusted Sources ○ High. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled. ○ Medium. You can choose whether or not to run potentially unsafe macros. ● Low (not recommended). You are not protected from potentially unsafe macros. Use this setting only if you have virus scanning software installed, or you are sure all documents you open are safe. No virus scanner installed. OK Cancel • Similarly lower the macro security for Microsoft Excel and Powerpoint.
Step 40: You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed. Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine. After you download the compatibility pack, install it on the virtual machine. To open files created by a later version of Microsoft Office applications, you must install the ,	

Step	Details
Step 41: In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **Continue.**	 Compatibility Pack for the 2007 Office system You must accept the Microsoft Software License Terms in orde MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT OFFICE COMPATIBILITY PACK FOR WORD, EXCE These license terms are an agreement between Microsoft Corp Please read them. They apply to the software named above, w also apply to any Microsoft • updates, • supplements, • Internet-based services, and • support services for this software, unless other terms accompany those items. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YO If you comply with these license terms, you have the rights be 1. INSTALLATION AND USE RIGHTS. You may install and use a 2. SCOPE OF LICENSE. The software is licensed, not sold. This reserves all other rights. Unless applicable law gives you more expressly permitted in this agreement. In doing so, you must c you to use it in certain ways. You may not • work around any technical limitations in the software; • reverse engineer, decompile or disassemble the software, exc this limitation; ☑ Click here to accept the Microsoft Software License Terms.

Step	Details
Step 42: To analyze PDF files, download Adobe Reader to the native host and copy it to the VM. This procedure uses Adobe Reader 9.0 as an example.	1 Install Adobe Reader 9.0 in the VM. 2 Open Adobe Reader and click **Accept**.  Adobe Reader - License Agreement Press the Accept button to agree to the Licer **ADOBE SYSTEMS INCORPORATED** **Warranty Disclaimer and Software License Agreement.** THIS DOCUMENT INCLUDES WARRANTY INFORMATION (PART THE USE OF ADOBE SOFTWARE (PART II). **PART I. WARRANTY DISCLAIMER.** THE SOFTWARE AND OTHER INFORMATION IS DELIVERED TO AND ITS SUPPLIERS AND CERTIFICATE AUTHORITIES DO NOT OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE, CER THIRD PARTY OFFERINGS. EXCEPT TO THE EXTENT ANY WARR TERM CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LA JURISDICTION, ADOBE AND ITS SUPPLIERS AND CERTIFICATE CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMP CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUD NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABI 3 a In Adobe Reader, select **Edit** | **Preferences** | **General** and deselect **Check for updates.** b In Adobe Reader, select **Help** | **Check for updates** | **Preferences** and deselect **Adobe Updates.**  Preferences Categories Documents Full Screen General Page Display 3D & Multimedia Accessibility Acrobat.com Forms Identity International Internet JavaScript Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Reading Search Security Security (Enhanced) Spelling Tracker Trust Manager Units Basic Tools ☐ Use single-key acce ☑ Create links from U ☐ Make Hand tool sel ☑ Make Hand tool rea ☐ Make Hand tool us ☐ Make Select tool se ☐ Use fixed resolution Warnings ☐ Do not show edit w Print ☑ Show page thumbn Application Startup ☐ Show splash screen ☐ Use only certified pl ☐ Check for updates
Step 43: To analyze JAR files, download and install Java Runtime Environment.	1 Goto https://community.mcafee.com/docs/DOC-6858. 2 Refer **Java installation guidance.docx**.

Step	Details
Step 44: Open Java in Control Panel.	 Control Panel ▸ Programs ▸ Control Panel Home System and Security Network and Internet Hardware and Sound Programs User Accounts and Family Safety Appearance and Personalization Clock, Language, and Region Ease of Access Programs anc Uninstall a progra Run programs ma Default Progr Change default se Make a file type a Desktop Gadg Add gadgets to th Restore desktop g Java (32-bit)
Step 45: In the **Update** tab, deselect **Check for Updates Automatically.**	 Java Control Panel The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied. Notify Me: Before downloading ☐ Check for Updates Automatically Click the "Update Now" button below to check for updates. An icon will appear in the system tray if an update is available. Move the cursor over the icon to see the status of the update.
Step 46: In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel.	 Java Update - Warning **You have chosen to stop automatically checking for updates and will miss future security updates.** We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.
Step 47: In the Windows Run dialog, enter `msconfig`.	 Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: msconfig This task will be created with administrative privileges.

Step	Details
Step 48: In the System Configuration utility, go to the **Startup** tab.	 System Configuration General Boot Services Startup Tools Startup Item — Manufacturer — Command — Location — Date □ Adobe Acrobat — Adobe System... — "C:\Program Fi... — HKLM\SOFTWARE\... □ Java(TM) Platform SE Auto Up... — Oracle Corpora... — "C:\Program Fi... — HKLM\SOFTWARE\... ☑ Microsoft Office XP — Microsoft Corp... — C:\PROGRA~2... — C:\ProgramData\Mic... Enable all Disable all OK Cancel Apply Help Deselect *reader_sl* and *jusched* and then click **OK**.
Step 49:: In the **System Configuration** dialog, click **Restart.**	 System Configuration You may need to restart your computer to apply these changes. Before restarting, save any open files and close all programs. □ Don't show this message again.

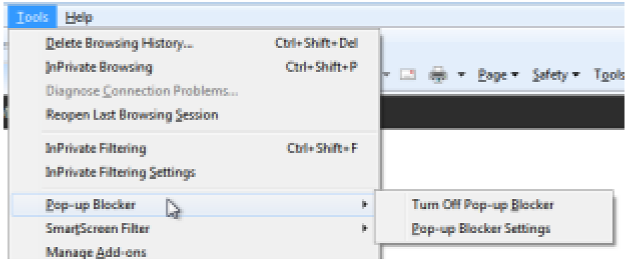
<table>
<tr><th>Step</th><th>Details</th></tr>
<tr><td>

Step 50: Open the default browser and set it up for malware analysis.

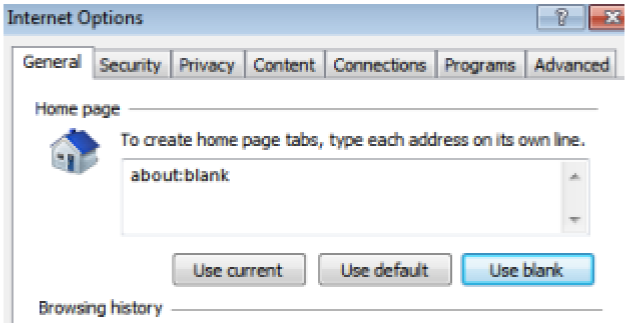
This procedure uses Internet Explorer as an example.

</td><td>

1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** | **Pop-up Blocker** | **Turn on Pop-up Blocker.**


Tools
Help
Delete Browsing History... Ctrl+Shift+Del
InPrivate Browsing Ctrl+Shift+P
Diagnose Connection Problems...
Reopen Last Browsing Session
InPrivate Filtering Ctrl+Shift+F
InPrivate Filtering Settings
Pop-up Blocker
SmartScreen Filter
Manage Add-ons
Turn Off Pop-up Blocker
Pop-up Blocker Settings
Page
Safety
Tools

2 Select **Tools** | **Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.

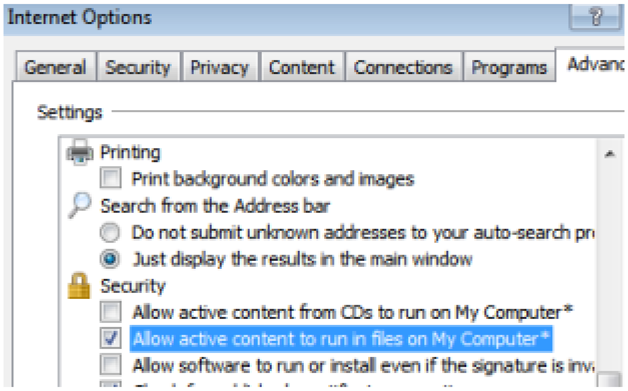


To create home page tabs, type each address on its own line.

about:blank

3 Go to the **Advanced** tab of the Internet Options and locate **Security.**

4 Select **Allow active content to run in files on My Computer.**



Printing
☐ Print background colors and images
Search from the Address bar
○ Do not submit unknown addresses to your auto-search pr
● Just display the results in the main window
Security
☐ Allow active content from CDs to run on My Computer*
☑ Allow active content to run in files on My Computer*
☐ Allow software to run or install even if the signature is inv

5 Click **OK.**

</td></tr>
<tr><td>

Step 51: To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.

</td><td>

1 Goto https://community.mcafee.com/docs/DOC-6859.

2 Refer **Adobe flash player installation guidance.docx.**

</td></tr>
</table>

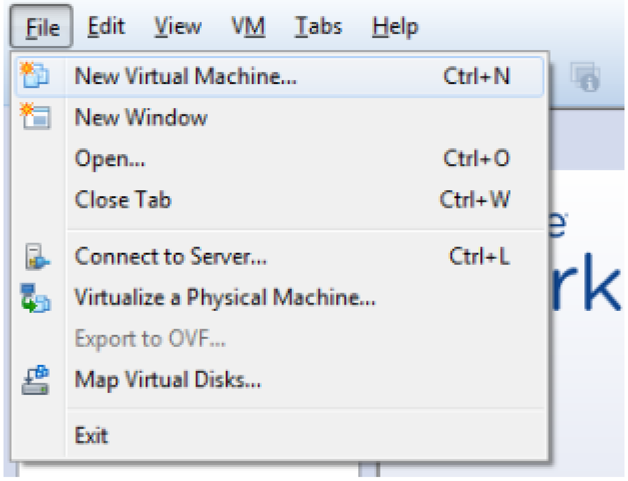
Step	Details
Step 52: Shut down virtualMachineImage by selecting **Start** | **Shut down.**	
Step 53: Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk`	

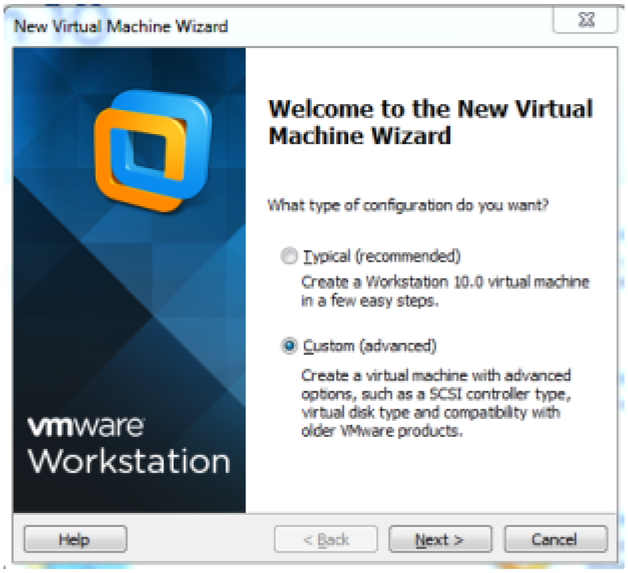
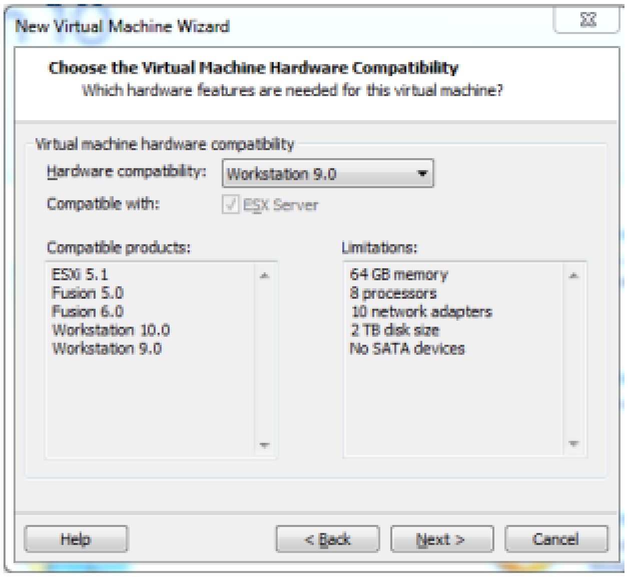
Create a VMDK file for Windows 2008 Server

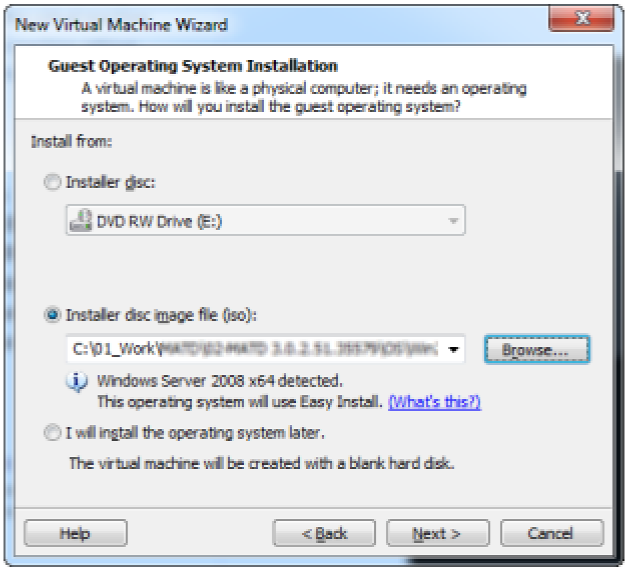
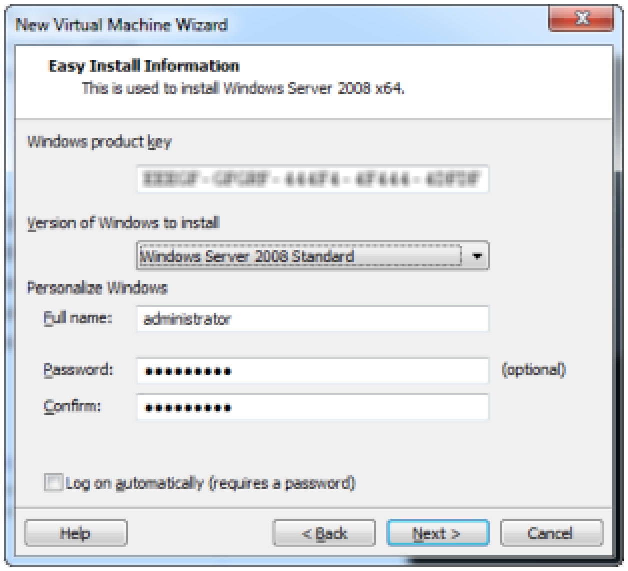
Before you begin

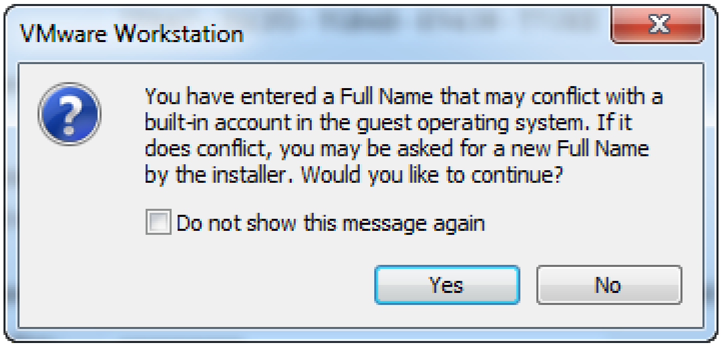
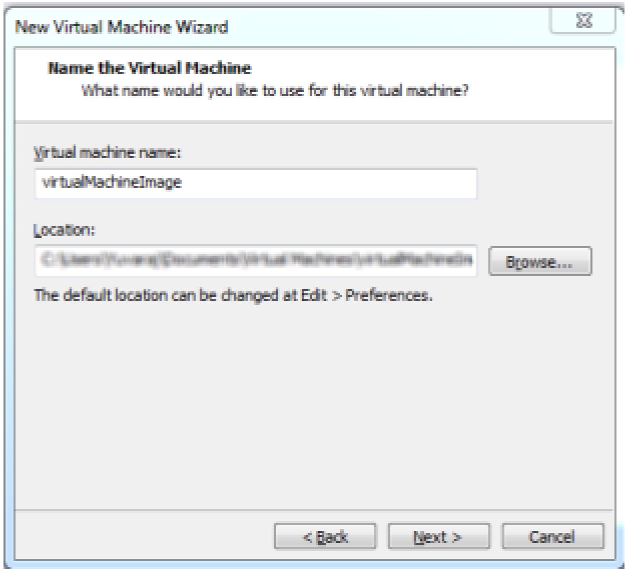
- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it.
- Make sure that you have the ISO image of Windows 2008 R2 SP1 for which you need to create the VMDK file. Only Windows 2008 64bit SP1 Standard is supported.
- Make sure you have the license key for the operating system.

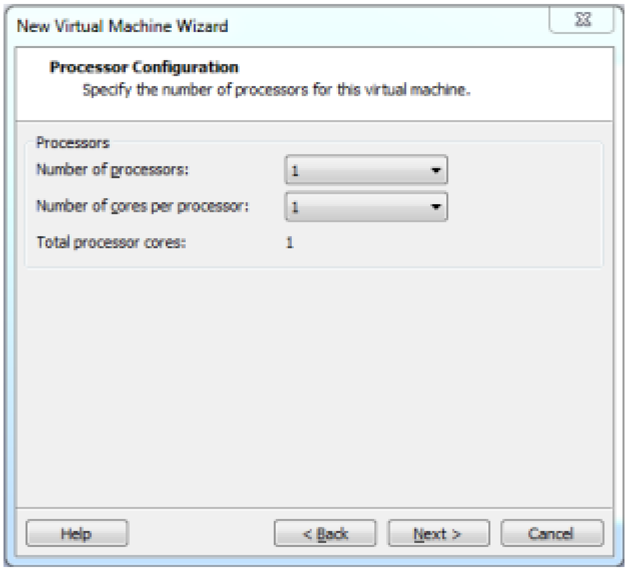
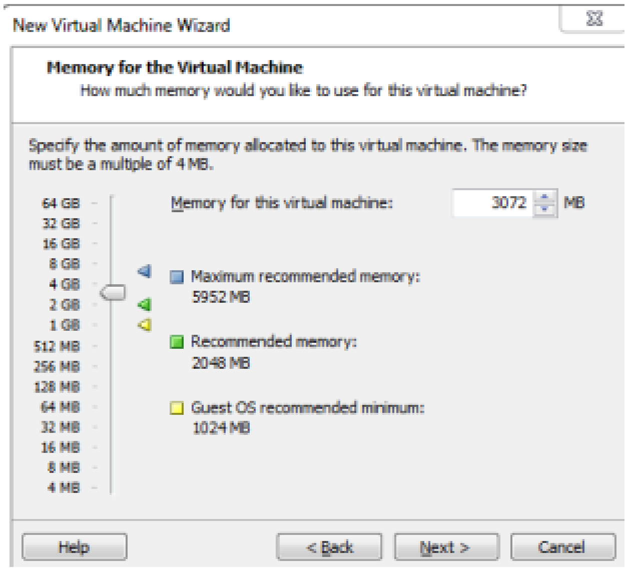
Use this procedure to create VMDK files from ISO images of Windows 2008 R2 SP1.

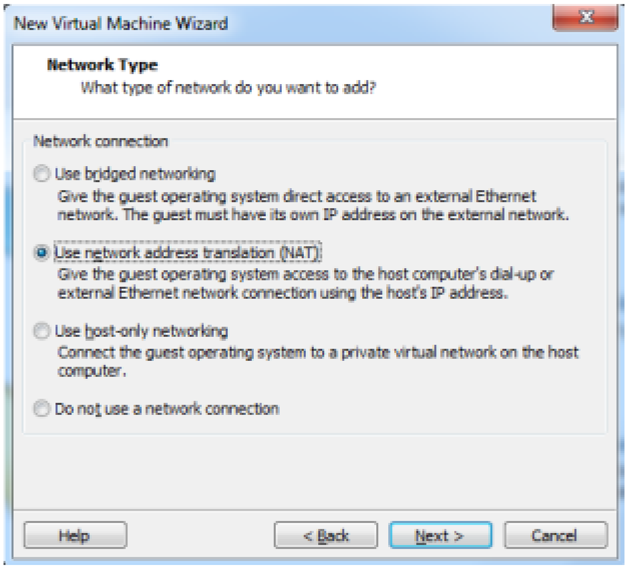
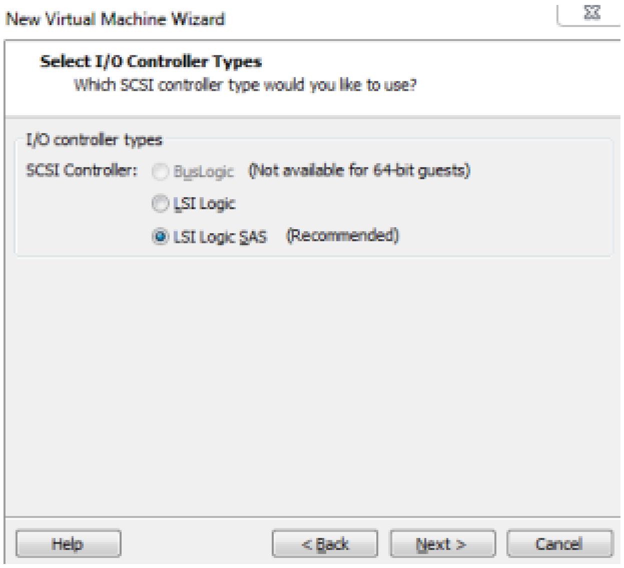
Step	Details
Step 1: Start the VMware Workstation.	This procedure uses VMware Workstation 10 as an example.
Step 2: In the VMware Workstation page, select **File** | **New Virtual Machine.**	 File Edit View VM Tabs Help New Virtual Machine... Ctrl+N New Window Open... Ctrl+O Close Tab Ctrl+W Connect to Server... Ctrl+L Virtualize a Physical Machine... Export to OVF... Map Virtual Disks... Exit

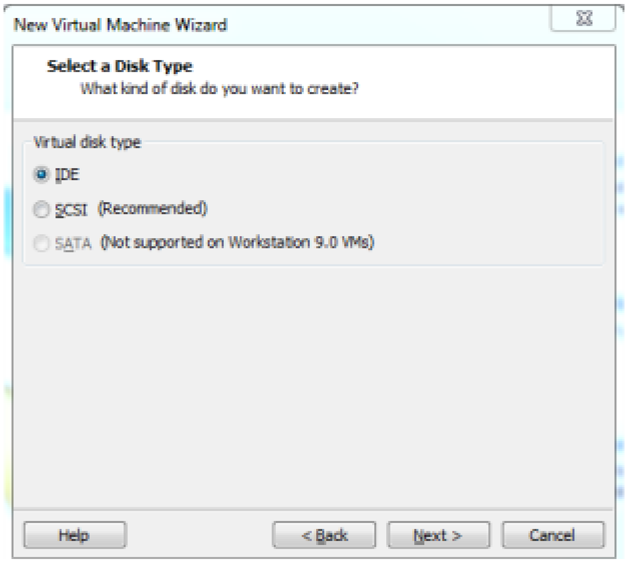
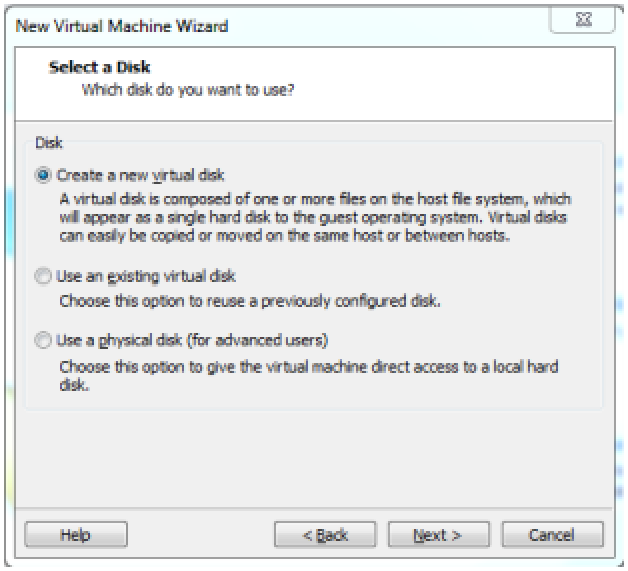
Step	Details
Step 3: In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.**	 New Virtual Machine Wizard Welcome to the New Virtual Machine Wizard What type of configuration do you want? ○ Typical (recommended) Create a Workstation 10.0 virtual machine in a few easy steps. ● Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Step 4: In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next.**	 New Virtual Machine Wizard Choose the Virtual Machine Hardware Compatibility Which hardware features are needed for this virtual machine? Virtual machine hardware compatibility Hardware compatibility: Workstation 9.0 Compatible with: ☑ ESX Server Compatible products: ESXi 5.1 Fusion 5.0 Fusion 6.0 Workstation 10.0 Workstation 9.0 Limitations: 64 GB memory 8 processors 10 network adapters 2 TB disk size No SATA devices

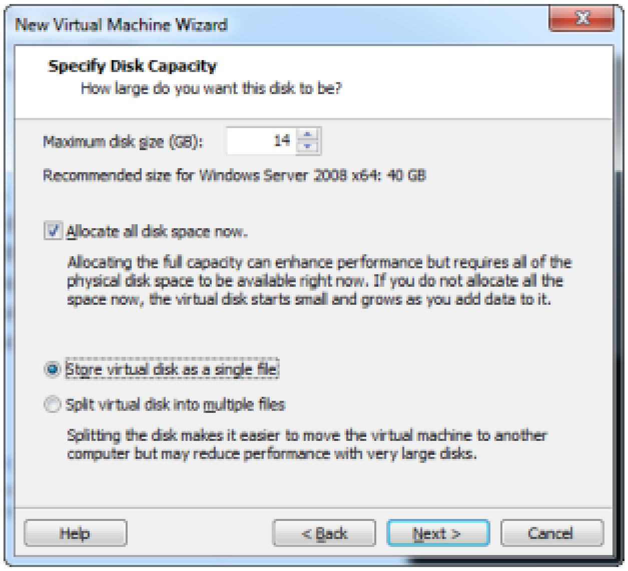
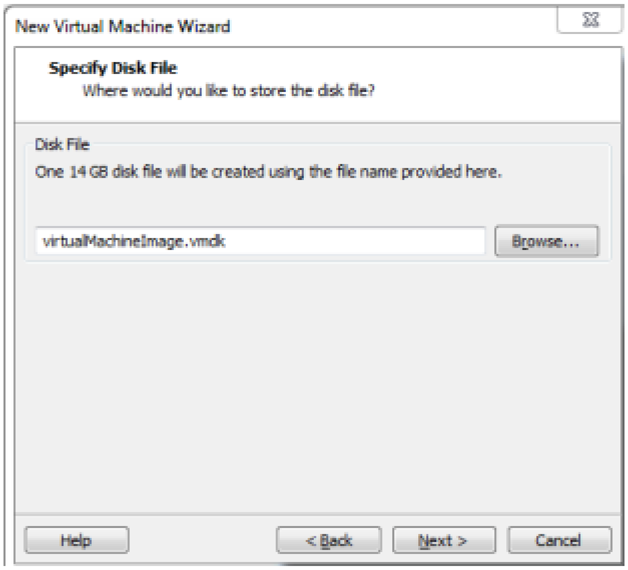
Step	Details
Step 5: In the **Guest Operating System Installation** window, select either **Installer disc** or **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next.**	 New Virtual Machine Wizard **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: ○ Installer disc: DVD RW Drive (E:) ● Installer disc image file (iso): C:\01_Work\[redacted] Browse... Windows Server 2008 x64 detected. This operating system will use Easy Install. (What's this?) ○ I will install the operating system later. The virtual machine will be created with a blank hard disk. Help · < Back · Next > · Cancel
Step 6: Enter the information in the **Easy Install Information** window and then click **Next**.	• **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file. • **Version of Windows to install** — Select the Standard version. • **Full name** — You must enter `administrator` as the **Full name.** • **Password** — You must enter `cr@cker42` as the password. This is the password that Advanced Threat Defense uses to log on to the VM. • **Confirm** — Enter `cr@cker42` again to confirm. • **Log on automatically (requires a password)** — Deselect this box.  New Virtual Machine Wizard **Easy Install Information** This is used to install Windows Server 2008 x64. Windows product key [redacted] Version of Windows to install Windows Server 2008 Standard Personalize Windows Full name: administrator Password: ••••••••• (optional) Confirm: ••••••••• ☐ Log on automatically (requires a password) Help · < Back · Next > · Cancel

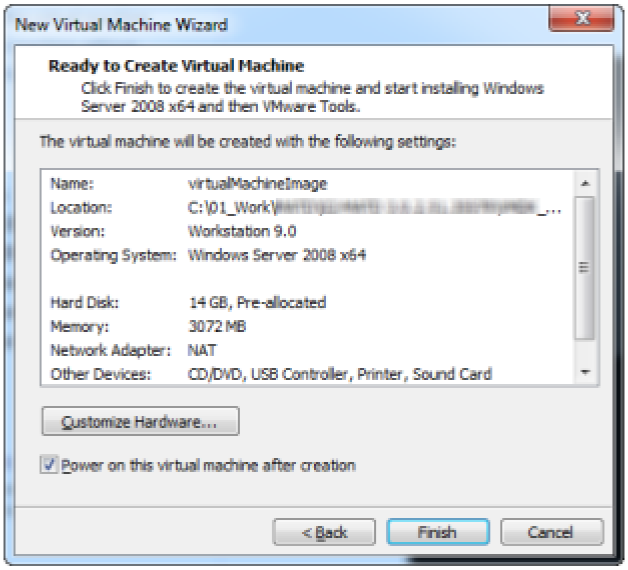
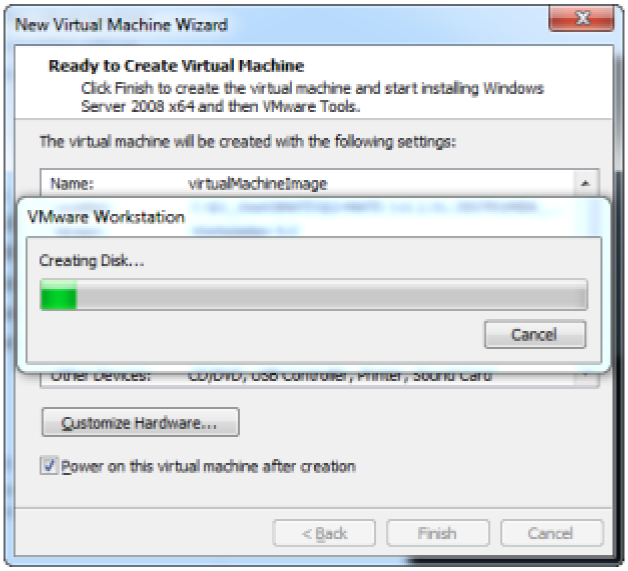
Step	Details
Step 7: If the **VMware Workstation** message displays, click **Yes**.	 VMware Workstation You have entered a Full Name that may conflict with a built-in account in the guest operating system. If it does conflict, you may be asked for a new Full Name by the installer. Would you like to continue? □ Do not show this message again Yes No
Step 8: Enter the information in the **Name the Virtual Machine** window and then click **Next**.	• **Virtual Machine name** — You must enter `virtualMachineImage` as the name. • **Location** — Browse and select the folder where you want to create the VMDK file.  New Virtual Machine Wizard **Name the Virtual Machine** What name would you like to use for this virtual machine? Virtual machine name: virtualMachineImage Location: [redacted] Browse... The default location can be changed at Edit > Preferences. < Back Next > Cancel

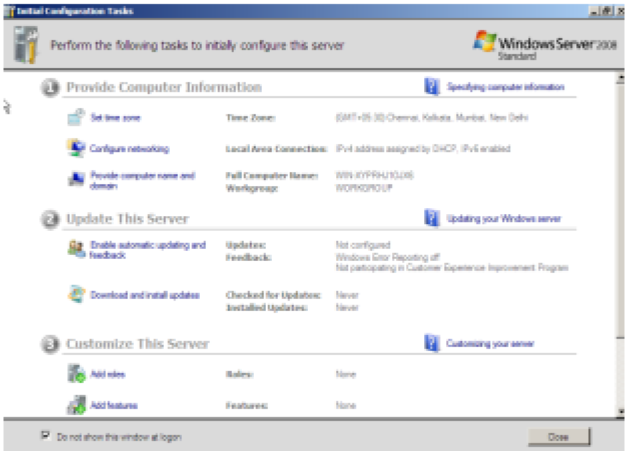
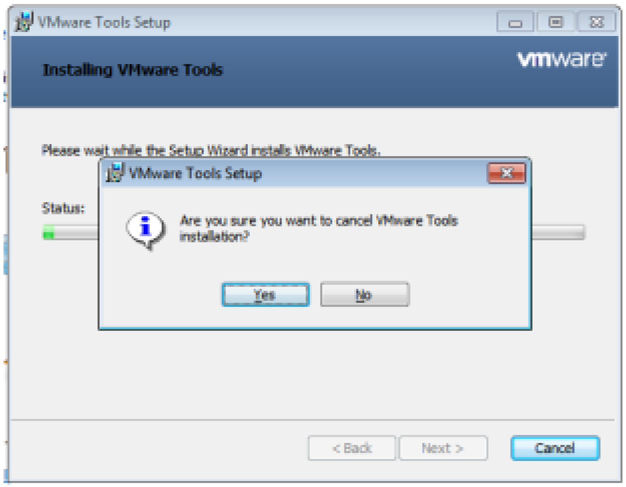
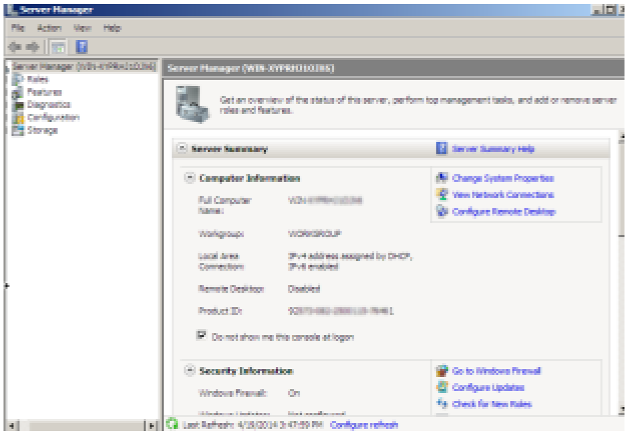
Step	Details
Step 9: In the **Processor Configuration** window, leave the default values and click **Next**.	 New Virtual Machine Wizard **Processor Configuration** Specify the number of processors for this virtual machine. Processors Number of processors: 1 Number of cores per processor: 1 Total processor cores: 1
Step 10: In the **Memory for the Virtual Machine** window, set 3072 MB as the memory.	 New Virtual Machine Wizard **Memory for the Virtual Machine** How much memory would you like to use for this virtual machine? Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB. Memory for this virtual machine: 3072 MB 🟦 Maximum recommended memory: 5952 MB 🟩 Recommended memory: 2048 MB 🟨 Guest OS recommended minimum: 1024 MB 64 GB 32 GB 16 GB 8 GB 4 GB 2 GB 1 GB 512 MB 256 MB 128 MB 64 MB 32 MB 16 MB 8 MB 4 MB Help < Back Next > Cancel

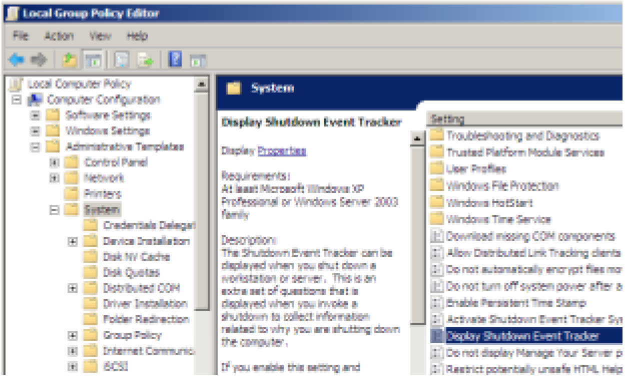
Step	Details
Step 11: In the **Network Type** window, leave the default selection.	 New Virtual Machine Wizard **Network Type** What type of network do you want to add? Network connection ○ Use bridged networking Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network. ● Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address. ○ Use host-only networking Connect the guest operating system to a private virtual network on the host computer. ○ Do not use a network connection
Step 12: In the **Select I/O Controller Types** , leave the default selection.	 New Virtual Machine Wizard **Select I/O Controller Types** Which SCSI controller type would you like to use? I/O controller types SCSI Controller: ○ BusLogic (Not available for 64-bit guests) ○ LSI Logic ● LSI Logic SAS (Recommended)

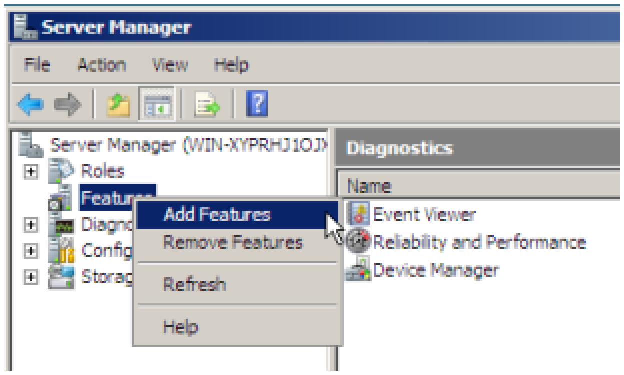
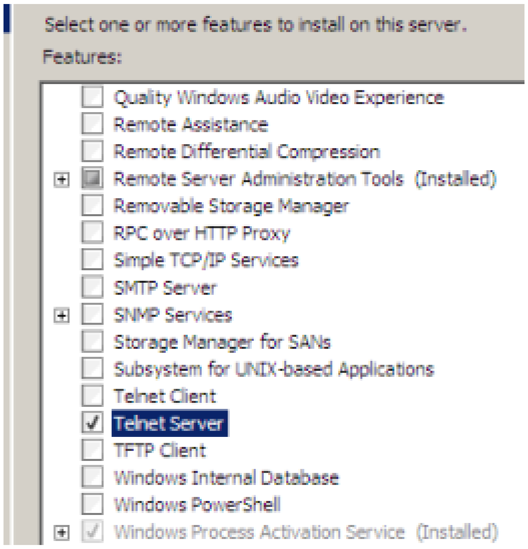
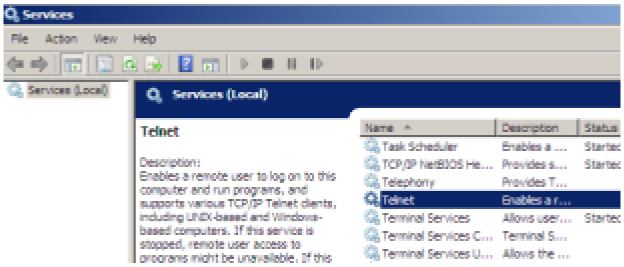
Step	Details
Step 13: In the **Select a Disk Type** page, select **IDE** and click **Next.** SCSI disks are not compatible with Advanced Threat Defense.	 New Virtual Machine Wizard Help < Back Next > Cancel **Select a Disk Type** What kind of disk do you want to create? Virtual disk type ● IDE ○ SCSI (Recommended) ○ SATA (Not supported on Workstation 9.0 VMs)
Step 14: In the **Select a Disk** window, select **Create a new virtual disk** and click **Next.**	 New Virtual Machine Wizard Help < Back Next > Cancel **Select a Disk** Which disk do you want to use? Disk ● Create a new virtual disk A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts. ○ Use an existing virtual disk Choose this option to reuse a previously configured disk. ○ Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard disk.

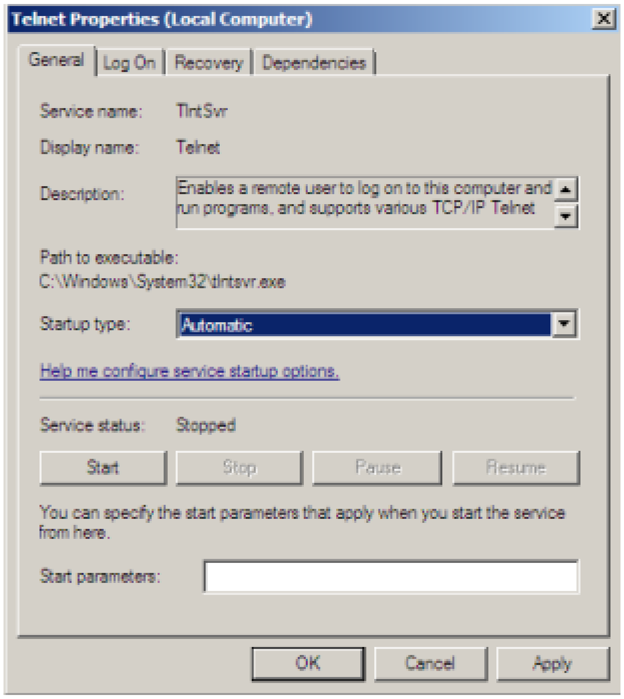
Step	Details
Step 15: Specify the details in the **Specify Disk Capacity** window and then click **Next**.	• **Maximum disk size (GB)** — For Windows 2008 Server, the maximum disk size can be 30 GB, however, you must enter 14 GB for optimal performance. • Select **Allocate all disk space now**. • Select **Store virtual disk as a single file**.  New Virtual Machine Wizard **Specify Disk Capacity** How large do you want this disk to be? Maximum disk size (GB): 14 Recommended size for Windows Server 2008 x64: 40 GB ☑ Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it. ● Store virtual disk as a single file ○ Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Step 16: In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**. If you specified a different name for **Virtual Machine name**, that name is displayed here.	 New Virtual Machine Wizard **Specify Disk File** Where would you like to store the disk file? Disk File One 14 GB disk file will be created using the file name provided here. virtualMachineImage.vmdk

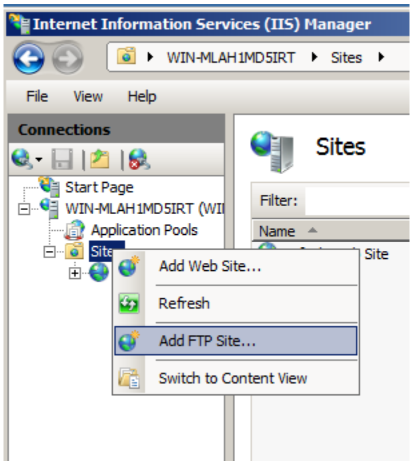
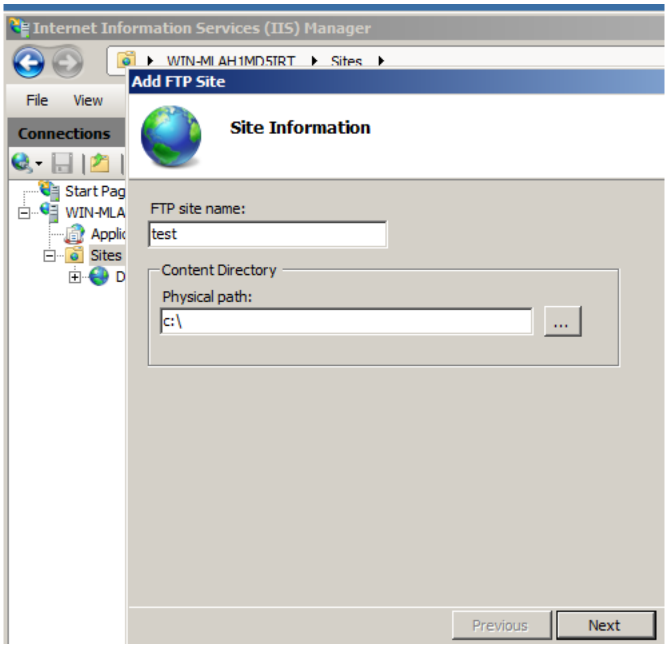
Step	Details
Step 17: Complete the following in the **Ready to Create Virtual Machine** window.	• **Power on this virtual machine after creation** — Select this option. • Click **Finish.** This step might take around 30 minutes to complete.  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows Server 2008 x64 and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage Location: C:\01_Work\[redacted]_... Version: Workstation 9.0 Operating System: Windows Server 2008 x64 Hard Disk: 14 GB, Pre-allocated Memory: 3072 MB Network Adapter: NAT Other Devices: CD/DVD, USB Controller, Printer, Sound Card ☑ Power on this virtual machine after creation  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows Server 2008 x64 and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage VMware Workstation Creating Disk... Other Devices: CD/DVD, USB Controller, Printer, Sound Card ☑ Power on this virtual machine after creation Cancel Customize Hardware... < Back Finish Cancel
Step 18: If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**.	Windows begins to install, which might take around 15 minutes.

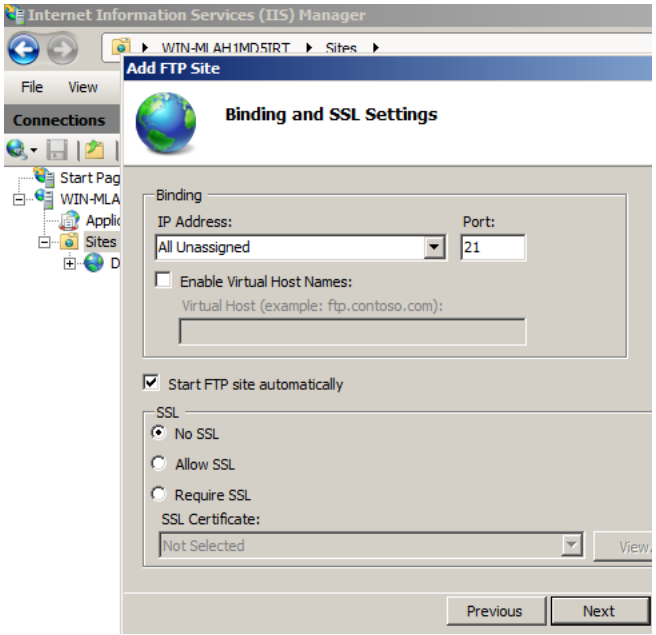
Step	Details
Step 19: If the **Initial Configuration Tasks** window is displayed, select **Do not show this window at logon** and click **Close**.	 Initial Configuration Tasks Perform the following tasks to initially configure this server Windows Server 2008 Standard 1 Provide Computer Information — Specifying computer information Set time zone — Time Zone: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi Configure networking — Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled Provide computer name and domain — Full Computer Name: WIN-XYPRHJ10JX6; Workgroup: WORKGROUP 2 Update This Server — Updating your Windows server Enable automatic updating and feedback — Updates: Not configured; Feedback: Windows Error Reporting off, Not participating in Customer Experience Improvement Program Download and install updates — Checked for Updates: Never; Installed Updates: Never 3 Customize This Server — Customizing your server Add roles — Roles: None Add features — Features: None ☑ Do not show this window at logon Close
Step 20: Stop the VMware Tools installation. The VMware Tools are not compatible with Advanced Threat Defense. If you did not stop the VMware Tools installation, you can continue with the VMDK file creation process but make sure it is uninstalled when the VMDK file is ready.	 VMware Tools Setup Installing VMware Tools Please wait while the Setup Wizard installs VMware Tools. Status: VMware Tools Setup Are you sure you want to cancel VMware Tools installation? Yes No < Back Next > Cancel
Step 21: If the **Server Manager** window is displayed, select **Do not show me this console at logon** and close the window.	 Server Manager File Action View Help Server Manager (WIN-XYPRHJ10JX6) Roles Features Diagnostics Configuration Storage Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features. Server Summary — Server Summary Help Computer Information Full Computer Name: [redacted] Workgroup: WORKGROUP Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled Remote Desktop: Disabled Product ID: [redacted] ☑ Do not show me this console at logon Change System Properties View Network Connections Configure Remote Desktop Security Information Windows Firewall: On Go to Windows Firewall Configure Updates Check for New Roles Last Refresh: 4/15/2014 3:47:59 PM Configure refresh

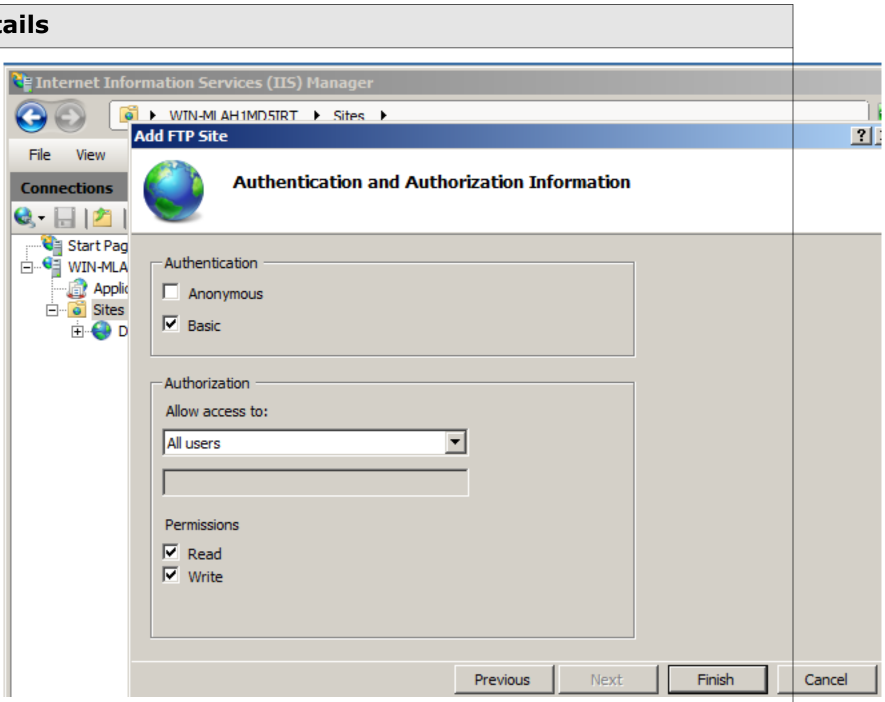
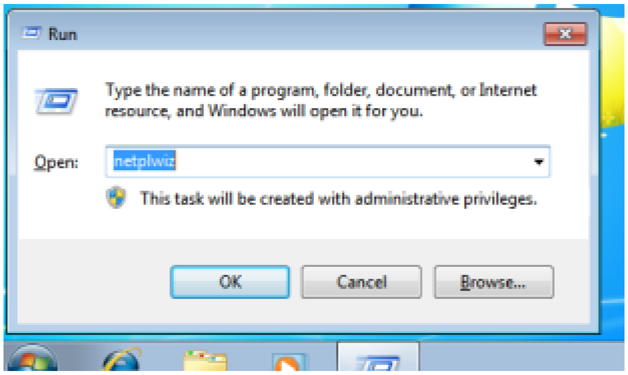
Step	Details
Step 22: Complete the following.	1 In the Windows Run window, enter `gpedit.msc` and press Enter. 2 In the **Local Group Policy Editor** window, select **Computer Configuration** | **Administrative Templates** | **System** and then double-click **Display Shutdown Event Tracker.**  Local Group Policy Editor File Action View Help Local Computer Policy Computer Configuration Software Settings Windows Settings Administrative Templates Control Panel Network Printers System Credentials Delegat Device Installation Disk NV Cache Disk Quotas Distributed COM Driver Installation Folder Redirection Group Policy Internet Communic iSCSI System Setting Troubleshooting and Diagnostics Trusted Platform Module Services User Profiles Windows File Protection Windows HotStart Windows Time Service Download missing COM components Allow Distributed Link Tracking clients Do not automatically encrypt files mo Do not turn off system power after a Enable Persistent Time Stamp Activate Shutdown Event Tracker Sy Display Shutdown Event Tracker Do not display Manage Your Server p Restrict potentially unsafe HTML HelpDisplay Shutdown Event Tracker Display Properties Requirements: At least Microsoft Windows XP Professional or Windows Server 2003 family Description: The Shutdown Event Tracker can be displayed when you shut down a workstation or server. This is an extra set of questions that is displayed when you invoke a shutdown to collect information related to why you are shutting down the computer. If you enable this setting and 3 In the **Display Shutdown Event Tracker Properties** dialog, select **Disabled** and click **OK.**
Step 23: In the VM, turn off the Windows Firewall.	1 Select **Start** | **Control Panel** | **Windows Firewall** | **Turn on Windows Firewall On or Off** 2 Select **Off** and then click **OK.**

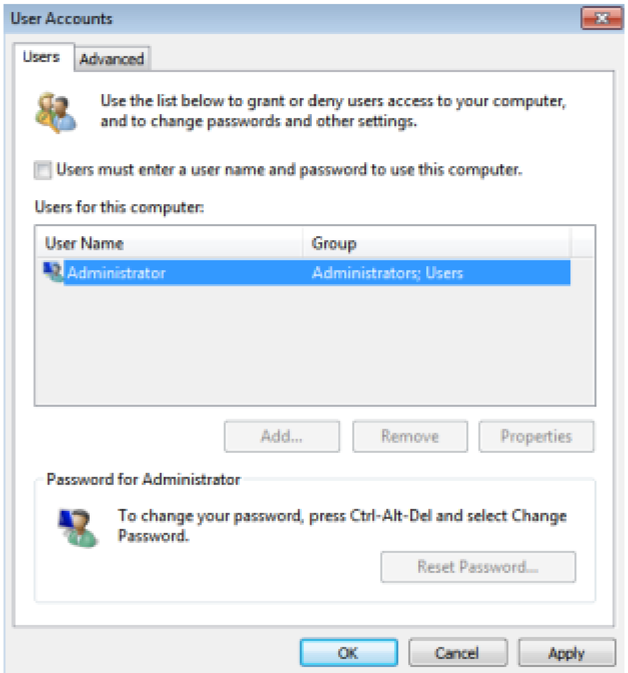
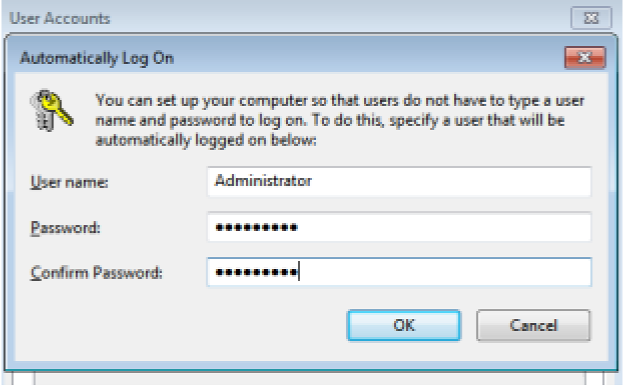
Step	Details
Step 24: Enable the Telnet feature.	1 In the virtualMachineImage, select **Start** | **Administrative Tools** | **Server Manager**. 2 In the **Server Manager** window, right-click **Features** and select **Add Features.**  Server Manager File Action View Help Server Manager (WIN-XYPRHJ1OJ Roles Features Diagno Config Storag Add Features Remove Features Refresh Help Diagnostics Name Event Viewer Reliability and Performance Device Manager 3 In the **Add Features Wizard**, select **Telnet Server.**  Select one or more features to install on this server. Features: ☐ Quality Windows Audio Video Experience ☐ Remote Assistance ☐ Remote Differential Compression ⊞ ▣ Remote Server Administration Tools (Installed) ☐ Removable Storage Manager ☐ RPC over HTTP Proxy ☐ Simple TCP/IP Services ☐ SMTP Server ⊞ ☐ SNMP Services ☐ Storage Manager for SANs ☐ Subsystem for UNIX-based Applications ☐ Telnet Client ☑ Telnet Server ☐ TFTP Client ☐ Windows Internal Database ☐ Windows PowerShell ⊞ ☑ Windows Process Activation Service (Installed) 4 Click **Next** and then **Install.** 5 Click **Close** after installation succeeds.
Step 25: Select **Start** | **Administrative Tools** | **Services**. Then double-click **Telnet.**	 Services File Action View Help Services (Local) Services (Local) Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this Name ^ | Description | Status Task Scheduler | Enables a ... | Startec TCP/IP NetBIOS He... | Provides s... | Startec Telephony | Provides T... | Telnet | Enables a r... | Terminal Services | Allows user... | Startec Terminal Services C... | Terminal S... | Terminal Services U... | Allows the ... |

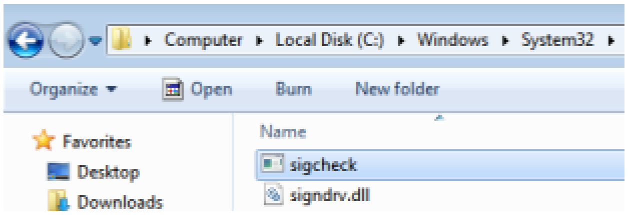
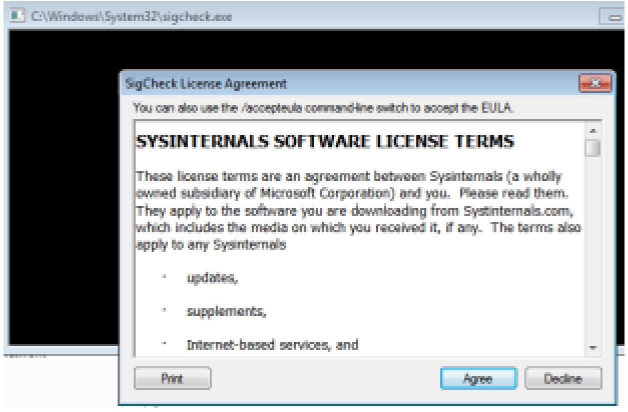
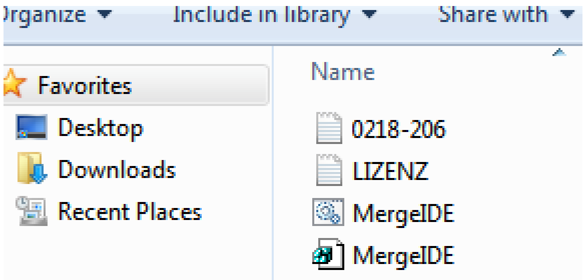
Step	Details
Step 26: In the Telnet Properties (Local Computer) dialog, select **Automatic** from the **Startup type** list. Then select **Apply** | **Start** | **OK**.	 Telnet Properties (Local Computer) General Log On Recovery Dependencies Start Stop Pause Resume OK Cancel Apply Service name: TlntSvr Display name: Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet Path to executable: C:\Windows\System32\tlntsvr.exe Startup type: Automatic Help me configure service startup options. Service status: Stopped You can specify the start parameters that apply when you start the service from here. Start parameters:

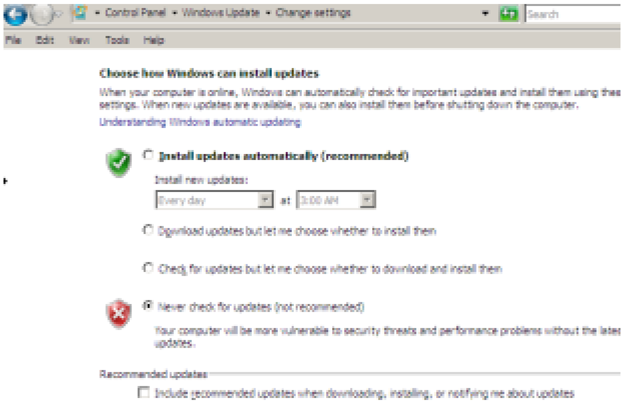
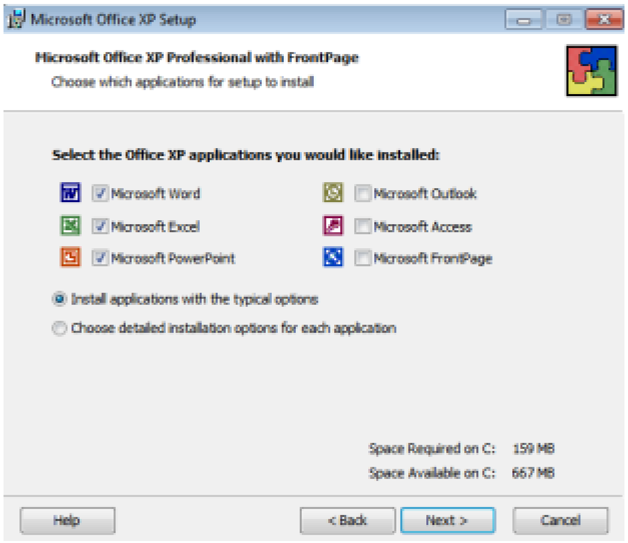
Step	Details
Step 27: Enable FTP on the VM.	1 In the virtualMachineImage, select **Start** | **Administrative Tools** | **Internet Information Services (IIS) Manager** 2 In the **Internet Information Services (IIS) Manager** window, select **Sites** | **Add FTP Site**  Internet Information Services (IIS) Manager WIN-MLAH1MD5IRT ▸ Sites ▸ File View Help Connections Start Page WIN-MLAH1MD5IRT (WI Application Pools Site Sites Filter: Name Site Add Web Site... Refresh Add FTP Site... Switch to Content View 3 a In the **Add FTP Site** wizard, enter **FTP site name** and **Physical path** and then click **Next**  Internet Information Services (IIS) Manager WIN-MLAH1MD5IRT ▸ Sites ▸ File View Connections Start Pag WIN-MLA Applic Sites D Add FTP Site Site Information Content Directory ... Previous Next FTP site name: test Physical path: c:\

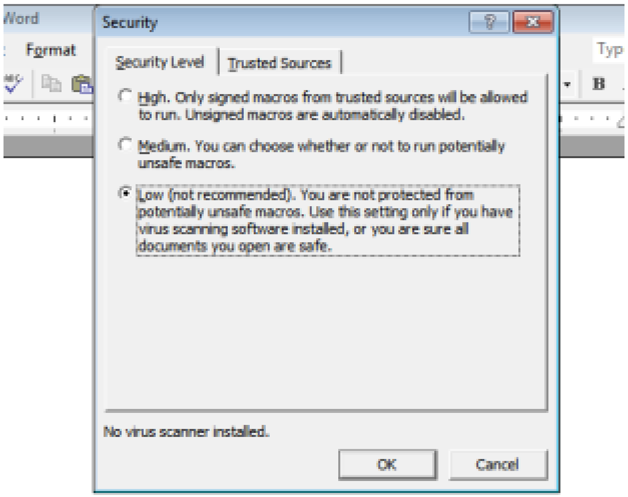
Step	Details
	b In the **Add FTP Site** wizard, enter the following under **Binding and SSL settings:** a **IP address** - Select **All Unassigned** - from the drop-down b **Port** - Enter the port number c Select **Start FTP site automatically** d Click **Next**  Internet Information Services (IIS) Manager WIN-MLAH1MD5IRT ▸ Sites ▸ Add FTP Site Binding and SSL Settings Binding IP Address: All Unassigned Port: 21 ☐ Enable Virtual Host Names: Virtual Host (example: ftp.contoso.com): ☑ Start FTP site automatically SSL ● No SSL ○ Allow SSL ○ Require SSL SSL Certificate: Not Selected File View Connections Start Pag WIN-MLA Applic Sites D View. Previous Next c In the **Add FTP Site** wizard, select required fields under **Authentication**, **Authorization** and **Permissions** and click **Finish**

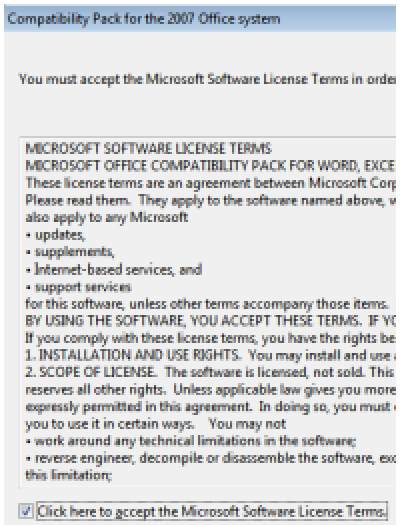
Step	Details
	 Internet Information Services (IIS) Manager WIN-MLAH1MD5IRT ▸ Sites ▸ File View Connections Start Pag WIN-MLA Applic Sites D Add FTP Site Previous Next Finish Cancel Authentication and Authorization Information Authentication ☐ Anonymous ☑ Basic Authorization Allow access to: All users Permissions ☑ Read ☑ Write
Step 28: select **Start** | **Run**, enter `netplwiz` and press **OK**.	 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: netplwiz This task will be created with administrative privileges.

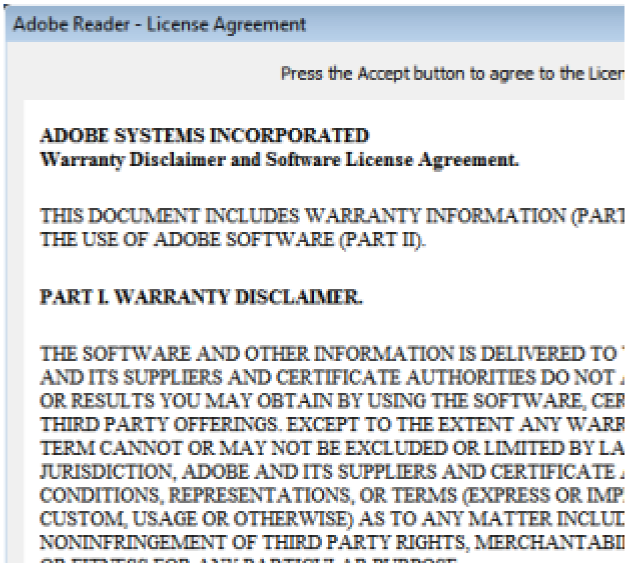
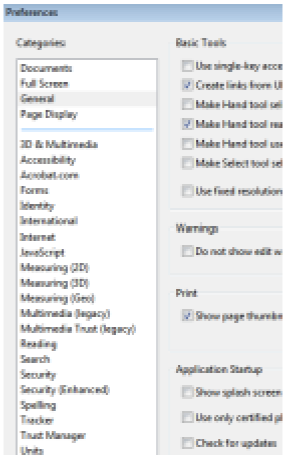
Step	Details
Step 29: In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply**.	 User Accounts Use the list below to grant or deny users access to your computer, and to change passwords and other settings. □ Users must enter a user name and password to use this computer. Users for this computer: User Name: Administrator — Group: Administrators; Users Password for Administrator To change your password, press Ctrl-Alt-Del and select Change Password. Users Advanced Add... Remove Properties Reset Password... OK Cancel Apply
Step 30: In the **Automatically Log On** pop-up window, complete the following and then press **OK** in the message boxes.	• **User name** — Enter `Administrator` • **Password** — Enter `cr@cker42` • **Confirm Password** — Enter `cr@cker42`  User Accounts Automatically Log On You can set up your computer so that users do not have to type a user name and password to log on. To do this, specify a user that will be automatically logged on below: User name: Administrator Password: ••••••••• Confirm Password: •••••••••
Step 31: Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx.	The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation.
Step 32: Extract sigcheck.zip to `C:\WINDOWS\system32` location.	

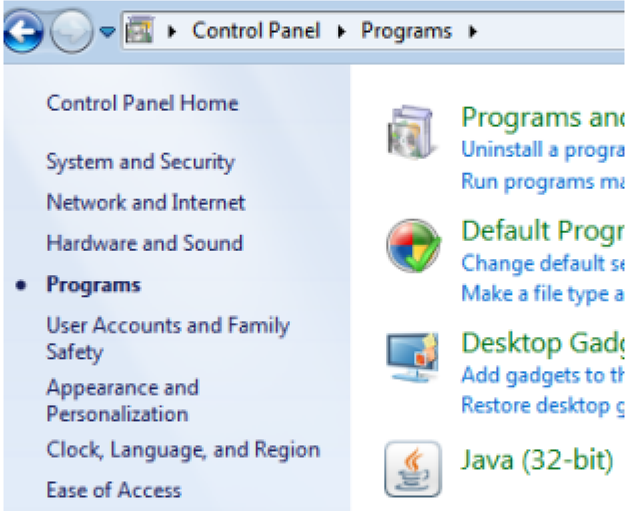
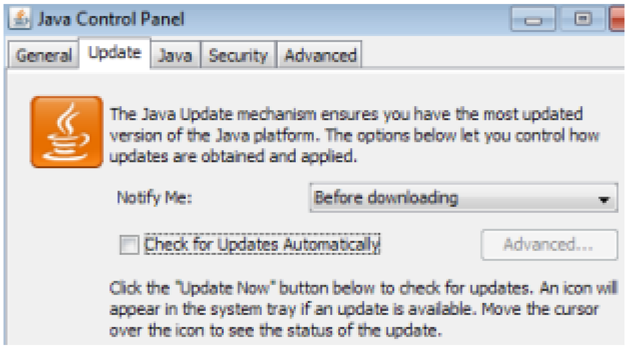
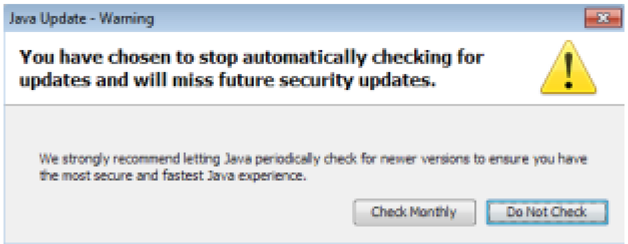
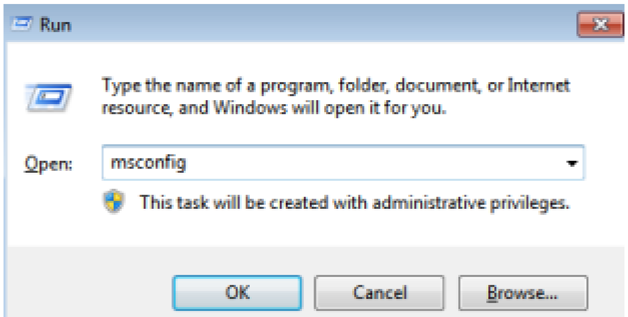
Step	Details
Step 33: In Windows Explorer, go to C:\ WINDOWS\system32 and double-click **sigcheck.exe**.	 Computer ▸ Local Disk (C:) ▸ Windows ▸ System32 ▸ Organize Open Burn New folder Favorites Desktop Downloads Name sigcheck signdrv.dll
Step 34 Click **Agree** for **Sigcheck License Agreement**. After you click on **Agree**, no confirmation message is displayed.	 C:\Windows\System32\sigcheck.exe SigCheck License Agreement You can also use the /accepteula command-line switch to accept the EULA. **SYSINTERNALS SOFTWARE LICENSE TERMS** These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals · updates, · supplements, · Internet-based services, and
Step 35: Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM.	)rganize Include in library Share with Favorites Desktop Downloads Recent Places Name 0218-206 LIZENZ MergeIDE MergeIDE
Step 36: Extract MergeIDE.zip and run the MergeIDE batch file in the VM.	• If prompted, select **Run** in the warning message. • Close Windows Explorer.

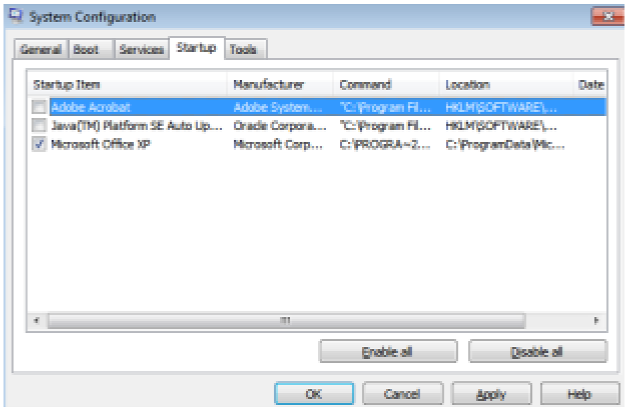
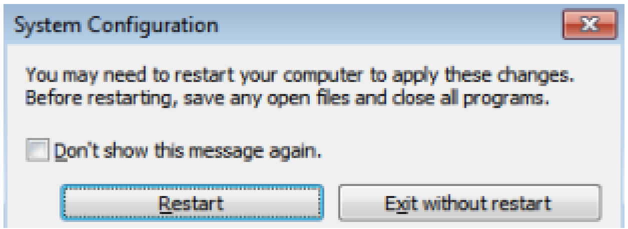
Step	Details
Step 37: Disable Windows updates.	1 Select **Start** | **Control Panel** | **Windows Update** | **Change settings.** 2 In the **Change settings** page, complete the following. a Select **Never check for updates (not recommended).** b Deselect the check box under **Recommended updates.**  Control Panel ▸ Windows Update ▸ Change settings File Edit View Tools Help **Choose how Windows can install updates** When your computer is online, Windows can automatically check for important updates and install them using thes settings. When new updates are available, you can also install them before shutting down the computer. Understanding Windows automatic updating ○ **Install updates automatically (recommended)** Install new updates: Every day at 3:00 AM ○ Download updates but let me choose whether to install them ○ Check for updates but let me choose whether to download and install them ● Never check for updates (not recommended) Your computer will be more vulnerable to security threats and performance problems without the lates updates. Recommended updates □ Include recommended updates when downloading, installing, or notifying me about updates 3 Click **OK.**
Step 38: To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine.	 Microsoft Office XP Setup **Microsoft Office XP Professional with FrontPage** Choose which applications for setup to install **Select the Office XP applications you would like installed:** ☑ Microsoft Word □ Microsoft Outlook ☑ Microsoft Excel □ Microsoft Access ☑ Microsoft PowerPoint □ Microsoft FrontPage ● Install applications with the typical options ○ Choose detailed installation options for each application Space Required on C: 159 MB Space Available on C: 667 MB Help < Back Next > Cancel

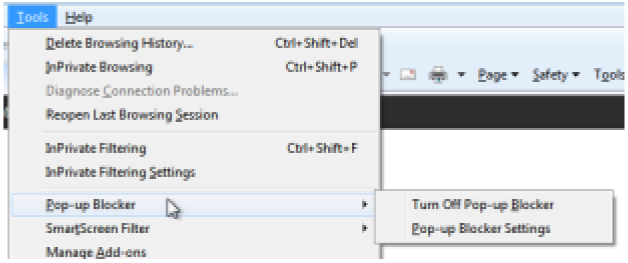
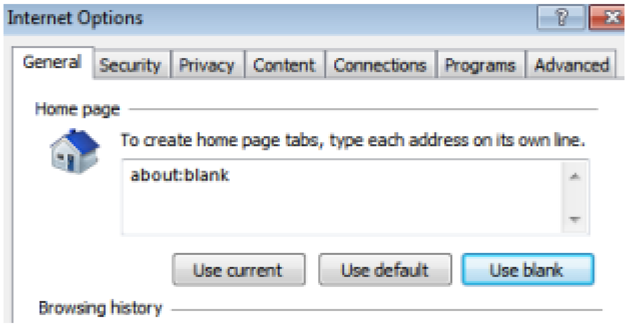
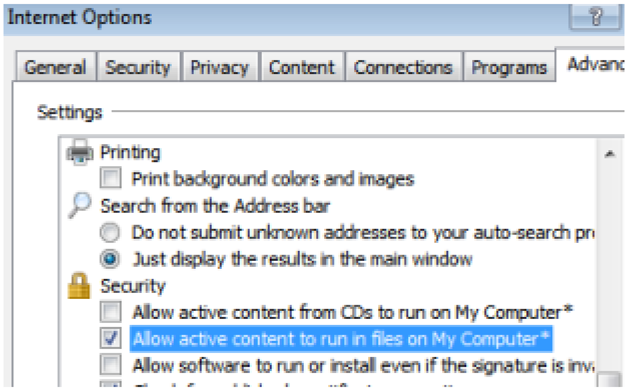
Step	Details
Step 39: Lower the security to run macros for the Office applications.	- Open Microsoft Word 2003 and select **Tools** | **Macro** | **Security** and then select **Low** and click **OK**.  Security Security Level | Trusted Sources ○ High. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled. ○ Medium. You can choose whether or not to run potentially unsafe macros. ● Low (not recommended). You are not protected from potentially unsafe macros. Use this setting only if you have virus scanning software installed, or you are sure all documents you open are safe. No virus scanner installed. OK Cancel - Similarly lower the macro security for Microsoft Excel and Powerpoint.
Step 40: You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed. Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine.	

Step	Details
Step 41: In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **Continue.**	 You must accept the Microsoft Software License Terms in orde MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT OFFICE COMPATIBILITY PACK FOR WORD, EXCE These license terms are an agreement between Microsoft Cor Please read them. They apply to the software named above, w also apply to any Microsoft • updates, • supplements, • Internet-based services, and • support services for this software, unless other terms accompany those items. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YC If you comply with these license terms, you have the rights be 1. INSTALLATION AND USE RIGHTS. You may install and use 2. SCOPE OF LICENSE. The software is licensed, not sold. This reserves all other rights. Unless applicable law gives you more expressly permitted in this agreement. In doing so, you must you to use it in certain ways. You may not • work around any technical limitations in the software; • reverse engineer, decompile or disassemble the software, exc this limitation; ☑ Click here to accept the Microsoft Software License Terms.

Step	Details
Step 42: To analyze PDF files, download Adobe Reader to the native host and copy it to the VM. This procedure uses Adobe Reader 9.0 as an example.	1 Install Adobe Reader 9.0 in the VM. 2 Open Adobe Reader and click **Accept**.  Adobe Reader - License Agreement Press the Accept button to agree to the Licen **ADOBE SYSTEMS INCORPORATED** **Warranty Disclaimer and Software License Agreement.** THIS DOCUMENT INCLUDES WARRANTY INFORMATION (PART THE USE OF ADOBE SOFTWARE (PART II). **PART I. WARRANTY DISCLAIMER.** THE SOFTWARE AND OTHER INFORMATION IS DELIVERED TO AND ITS SUPPLIERS AND CERTIFICATE AUTHORITIES DO NOT OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE, CER THIRD PARTY OFFERINGS. EXCEPT TO THE EXTENT ANY WARR TERM CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LA JURISDICTION, ADOBE AND ITS SUPPLIERS AND CERTIFICATE CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMP CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUD NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABI 3 a In Adobe Reader, select **Edit** | **Preferences** | **General** and deselect **Check for updates.** b In Adobe Reader, select **Help** | **Check for updates** | **Preferences** and deselect **Adobe Updates.**  Preferences Categories: Documents, Full Screen, General, Page Display, 3D & Multimedia, Accessibility, Acrobat.com, Forms, Identity, International, Internet, JavaScript, Measuring (2D), Measuring (3D), Measuring (Geo), Multimedia (legacy), Multimedia Trust (legacy), Reading, Search, Security, Security (Enhanced), Spelling, Tracker, Trust Manager, Units Basic Tools ☐ Use single-key acce ☑ Create links from U ☐ Make Hand tool sel ☑ Make Hand tool rea ☐ Make Hand tool us ☐ Make Select tool se ☐ Use fixed resolution Warnings ☐ Do not show edit w Print ☑ Show page thumbn Application Startup ☐ Show splash screen ☐ Use only certified pl ☐ Check for updates
Step 43: To analyze JAR files, download and install Java Runtime Environment.	1 Goto https://community.mcafee.com/docs/DOC-6858. 2 Refer **Java installation guidance.docx**.

Step	Details
Step 44: Open Java in Control Panel.	 Control Panel ▸ Programs ▸ Control Panel Home System and Security Network and Internet Hardware and Sound Programs User Accounts and Family Safety Appearance and Personalization Clock, Language, and Region Ease of Access Programs anc Uninstall a progra Run programs ma Default Progr Change default se Make a file type a Desktop Gad Add gadgets to th Restore desktop g Java (32-bit)
Step 45: In the **Update** tab, deselect **Check for Updates Automatically.**	 The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied. Notify Me: Before downloading ☐ Check for Updates Automatically Click the "Update Now" button below to check for updates. An icon will appear in the system tray if an update is available. Move the cursor over the icon to see the status of the update.
Step 46: In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel.	 **You have chosen to stop automatically checking for updates and will miss future security updates.** We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.
Step 47: In the Windows Run dialog, enter `msconfig`.	 Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: msconfig This task will be created with administrative privileges.

Step	Details
Step 48: In the System Configuration utility, go to the **Startup** tab.	 System Configuration General Boot Services Startup Tools Enable all Disable all OK Cancel Apply Help Startup Item | Manufacturer | Command | Location | Date ☐ Adobe Acrobat | Adobe System... | "C:\Program Fil... | HKLM\SOFTWARE\... ☐ Java(TM) Platform SE Auto Up... | Oracle Corpora... | "C:\Program Fil... | HKLM\SOFTWARE\... ☑ Microsoft Office XP | Microsoft Corp... | C:\PROGRA~2... | C:\ProgramData\Mic... Deselect all the items and click **OK**.
Step 49: In the **System Configuration** dialog, select **Don't show this message again** and click **Restart.**	 System Configuration You may need to restart your computer to apply these changes. Before restarting, save any open files and close all programs. ☐ Don't show this message again.

Step	Details
Step 50: Open the default browser and set it up for malware analysis. This procedure uses Internet Explorer as an example.	1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools | Pop-up Blocker | Turn on Pop-up Blocker.**  Tools Help Delete Browsing History... Ctrl+Shift+Del InPrivate Browsing Ctrl+Shift+P Diagnose Connection Problems... Reopen Last Browsing Session InPrivate Filtering Ctrl+Shift+F InPrivate Filtering Settings Pop-up Blocker SmartScreen Filter Manage Add-ons Turn Off Pop-up Blocker Pop-up Blocker Settings Page Safety Tools 2 Select **Tools | Internet Options** and for **Home page** select **Use Blank** or **Use new tab** based on the version of Internet Explorer.  Internet Options Home page To create home page tabs, type each address on its own line. about:blank General Security Privacy Content Connections Programs Advanced Use current Use default Use blank Browsing history 3 Go to the **Advanced** tab of the Internet Options and locate **Security.** 4 Select **Allow active content to run in files on My Computer.**  Internet Options Settings Printing ☐ Print background colors and images Search from the Address bar ○ Do not submit unknown addresses to your auto-search pr ● Just display the results in the main window Security ☐ Allow active content from CDs to run on My Computer* ☑ Allow active content to run in files on My Computer* ☐ Allow software to run or install even if the signature is inv General Security Privacy Content Connections Programs Advanc 5 Click **OK.**
Step 51: To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.	1 Goto https://community.mcafee.com/docs/DOC-6859. 2 Refer **Adobe flash player installation guidance.docx**.

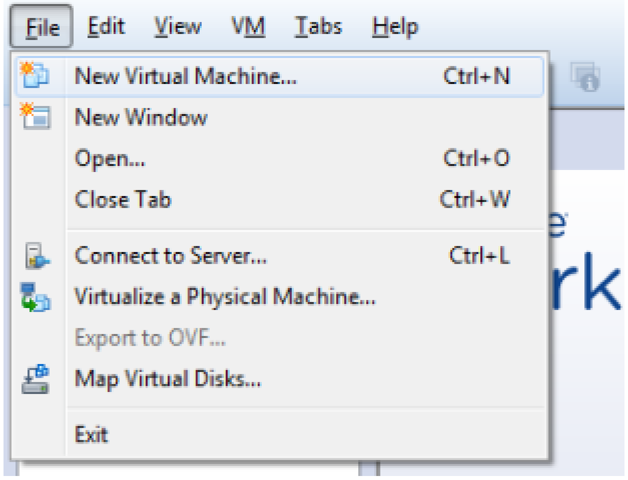
Step	Details
Step 52: Shut down virtualMachineImage by selecting **Start | Shut down.**	
Step 53: Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk`	

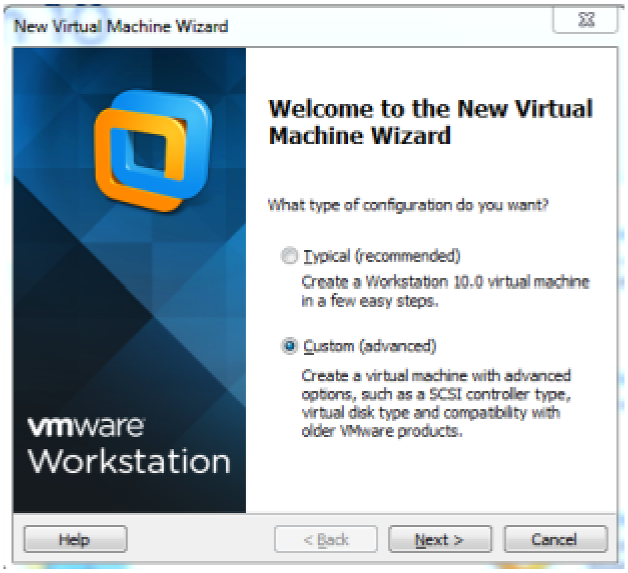
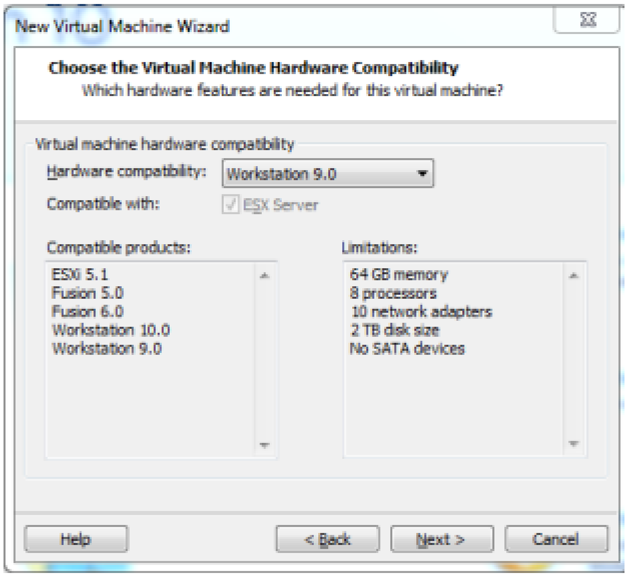
Create a VMDK file for Windows 8

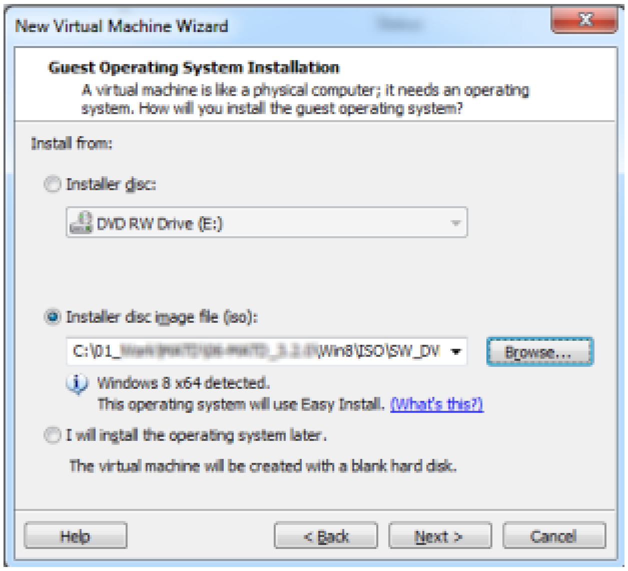
Before you begin

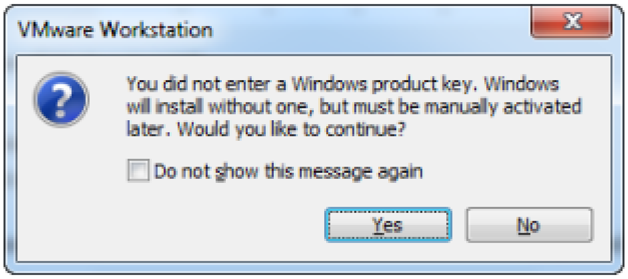
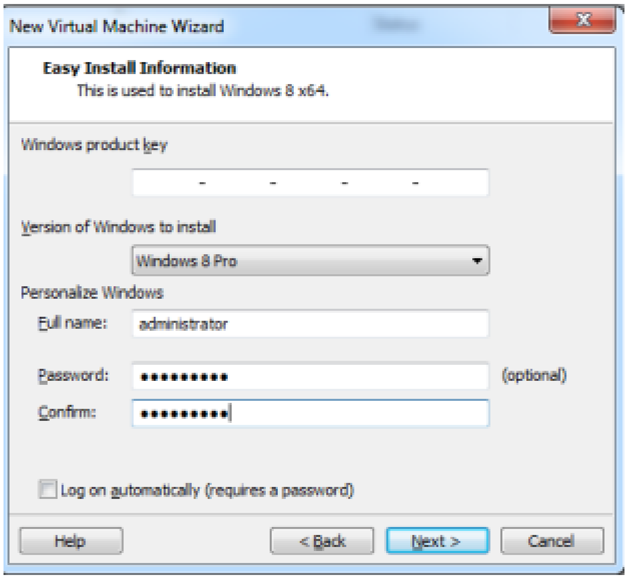
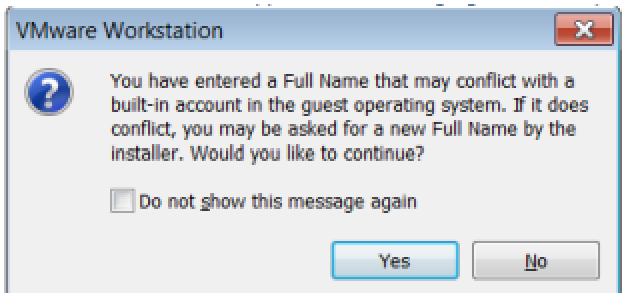
- Download VMware Workstation 9.0 or above from http://www.vmware.com/products/workstation/workstation-evaluation and install it. McAfee recommends version 9 or 10.
- Make sure that you have the ISO image of Windows 8 32-bit or 64-bit for which you need to create the VMDK file. Only Windows 8 Pro is supported. This procedure uses Windows 8 Pro English version as an example.
- Make sure you have the details to activate the operating system based on the type of license you possess. You must activate the operating system before you import the VMDK file into Advanced Threat Defense.

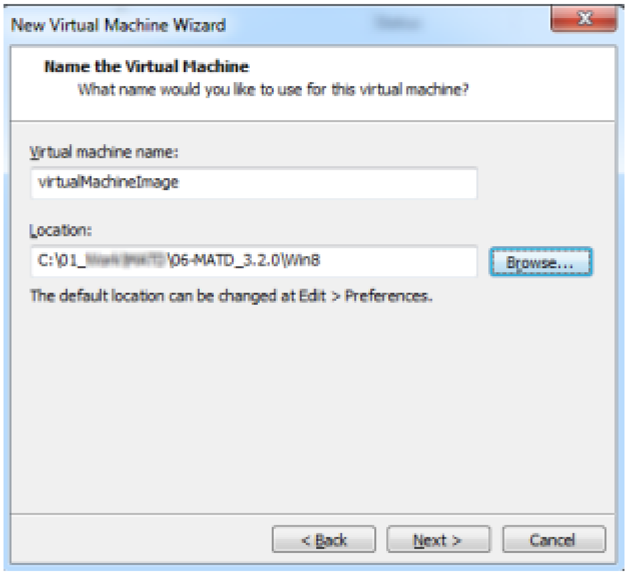
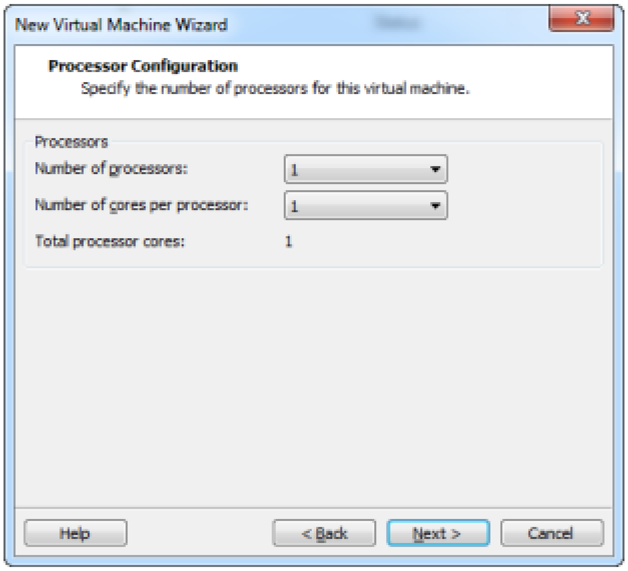
Use this procedure to create VMDK files from an ISO image of Windows 8 Pro 32 bit or 64 bit.

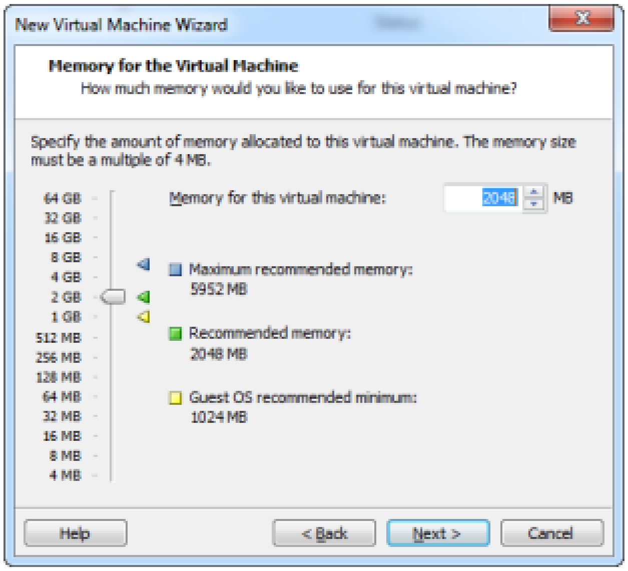
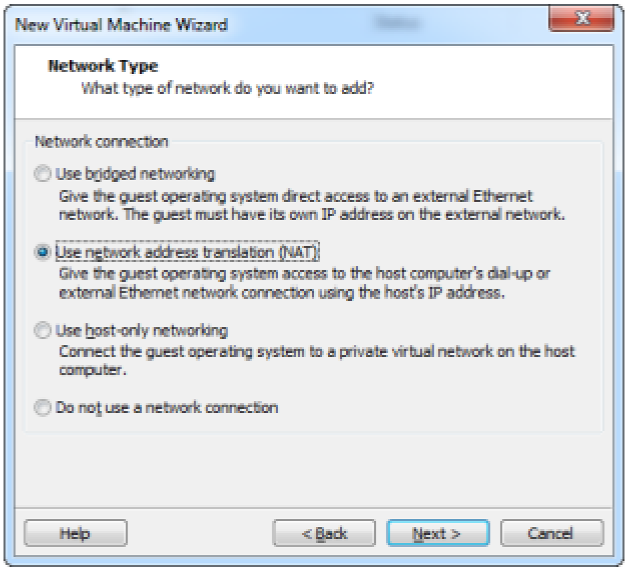
Step	Details
Step 1: Start the VMware Workstation.	This procedure uses VMware Workstation 10 as an example.
Step 2: In the VMware Workstation page, select **File | New Virtual Machine.**	 File Edit View VM Tabs Help New Virtual Machine... Ctrl+N New Window Open... Ctrl+O Close Tab Ctrl+W Connect to Server... Ctrl+L Virtualize a Physical Machine... Export to OVF... Map Virtual Disks... Exit

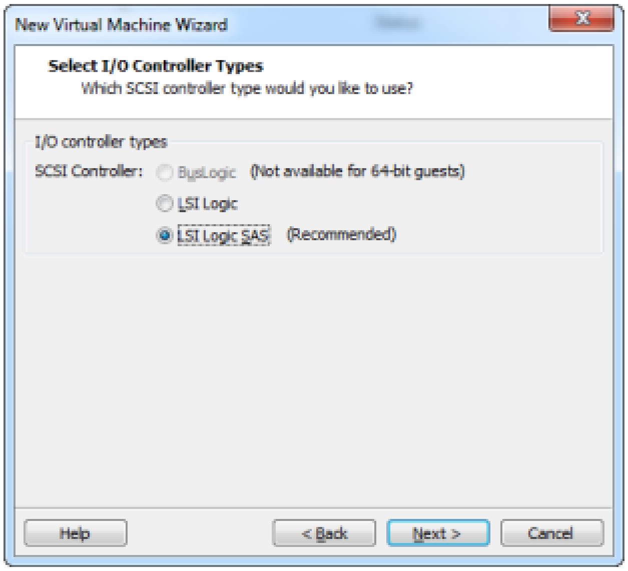
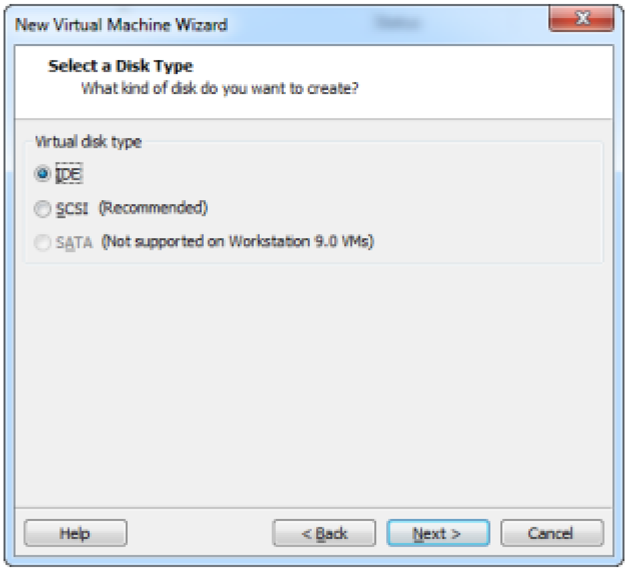
Step	Details
Step 3: In the **New Virtual Machine Wizard** window, select **Custom (Advanced)** and click **Next.**	 New Virtual Machine Wizard Welcome to the New Virtual Machine Wizard What type of configuration do you want? ○ Typical (recommended) Create a Workstation 10.0 virtual machine in a few easy steps. ● Custom (advanced) Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.
Step 4: In the **Choose the Virtual Machine Hardware Compatibility** window, select **Workstation 9.0** from the **Hardware compatibility** drop-down list. For other fields, leave the default values and click **Next.**	 New Virtual Machine Wizard Choose the Virtual Machine Hardware Compatibility Which hardware features are needed for this virtual machine? Virtual machine hardware compatibility Hardware compatibility: Workstation 9.0 Compatible with: ☑ ESX Server Compatible products: ESXi 5.1 Fusion 5.0 Fusion 6.0 Workstation 10.0 Workstation 9.0 Limitations: 64 GB memory 8 processors 10 network adapters 2 TB disk size No SATA devices

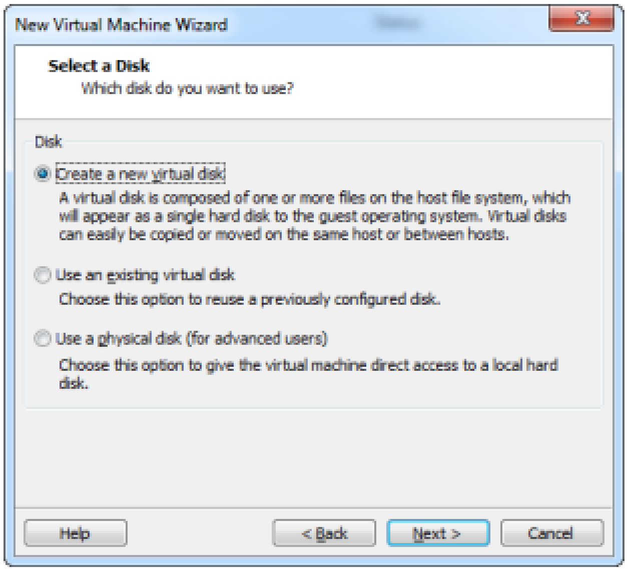
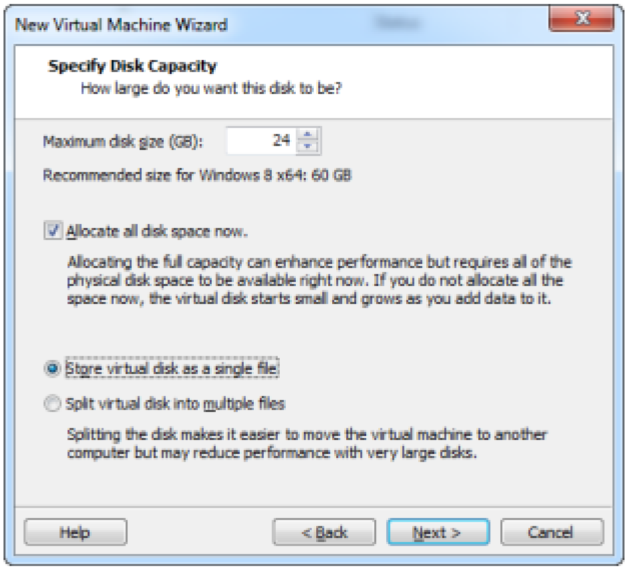
Step	Details
Step 5: In the **Guest Operating System Installation** window, select **Installer disc image file (iso)**, browse and select the ISO image, and then click **Next.**	 New Virtual Machine Wizard [redacted] **Guest Operating System Installation** A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system? Install from: ○ Installer disc: DVD RW Drive (E:) ● Installer disc image file (iso): C:\01_[redacted]\Win8\ISO\SW_DV Windows 8 x64 detected. This operating system will use Easy Install. (What's this?) ○ I will install the operating system later. The virtual machine will be created with a blank hard disk.

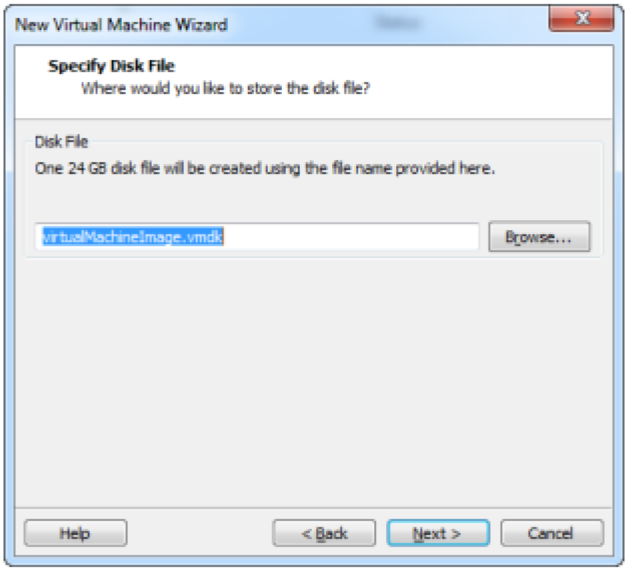
Step	Details
Step 6: Enter the information in the **Easy Install Information** window and then click **Next**.	- **Windows product key** — Enter the license key of the Windows operating system for which you are creating the VMDK file. For volume license, you can leave it empty. Click **Yes** if the following message is displayed subsequently.  VMware Workstation You did not enter a Windows product key. Windows will install without one, but must be manually activated later. Would you like to continue? □ Do not show this message again - **Full name** — Enter `administrator` as the **Full name.** - **Password** — Enter `cr@cker42` as the password. Advanced Threat Defense uses this password to log on to the VM. - **Confirm** — Enter `cr@cker42` again to confirm. - **Log on automatically (requires a password)** — Deselect this box.  New Virtual Machine Wizard Easy Install Information This is used to install Windows 8 x64. Windows product key: - - - - Version of Windows to install: Windows 8 Pro Personalize Windows Full name: administrator Password: ••••••••• (optional) Confirm: ••••••••• □ Log on automatically (requires a password)
Step 7: If the **VMware Workstation** message displays, click **Yes**.	 VMware Workstation You have entered a Full Name that may conflict with a built-in account in the guest operating system. If it does conflict, you may be asked for a new Full Name by the installer. Would you like to continue? □ Do not show this message again

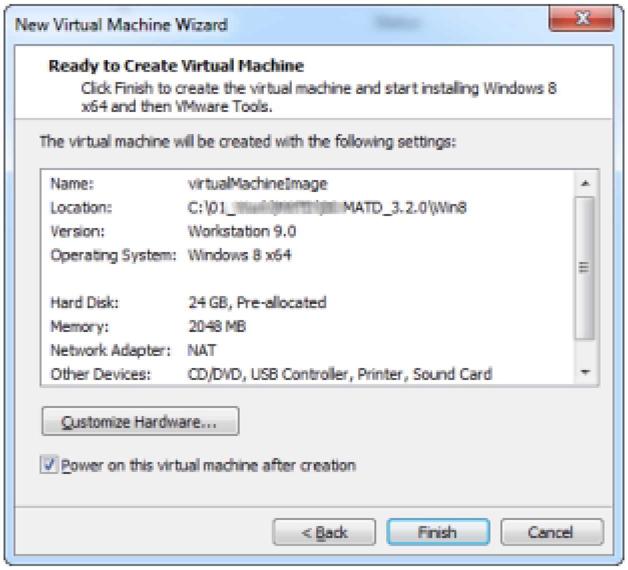
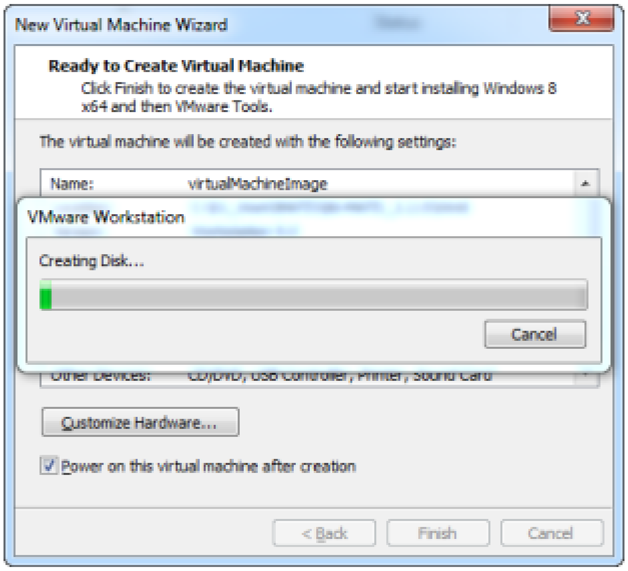
Step	Details
Step 8: Enter the information in the **Name the Virtual Machine** window and then click **Next**.	- **Virtual Machine name** — You must enter `virtualMachineImage` as the name. - **Location** — Browse and select the folder where you want to create the VMDK file.  New Virtual Machine Wizard [redacted] **Name the Virtual Machine** What name would you like to use for this virtual machine? Virtual machine name: virtualMachineImage Location: C:\01_[redacted]\06-MATD_3.2.0\Win8 The default location can be changed at Edit > Preferences.
Step 9: In the **Processor Configuration** window, leave the default values and click **Next**.	 New Virtual Machine Wizard [redacted] **Processor Configuration** Specify the number of processors for this virtual machine. Processors Number of processors: 1 Number of cores per processor: 1 Total processor cores: 1

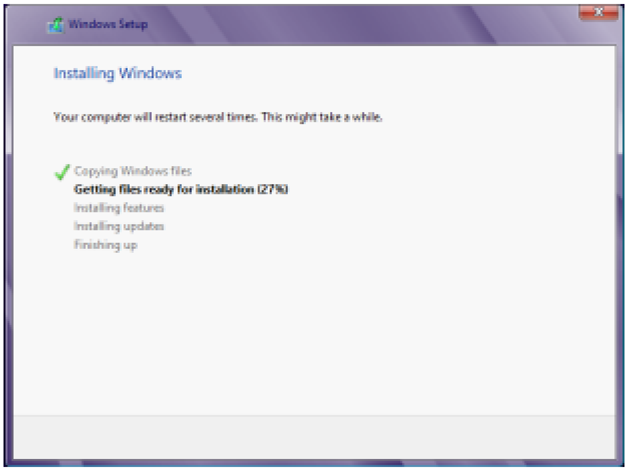
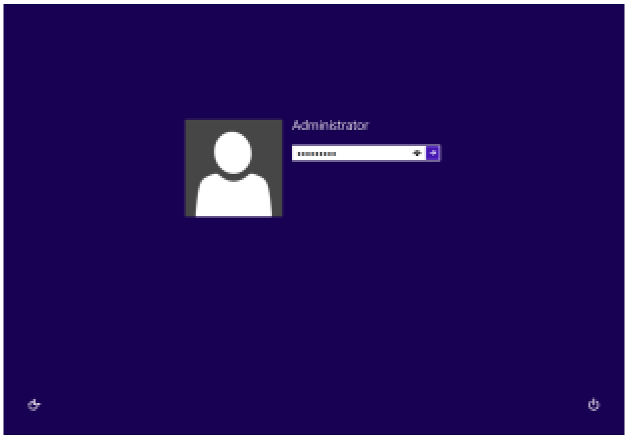
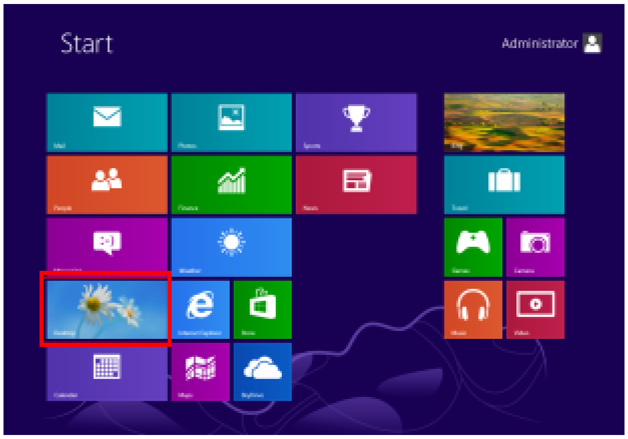
Step	Details
Step 10: In the **Memory for the Virtual Machine** window, set 2048 MB as the memory.	 New Virtual Machine Wizard **Memory for the Virtual Machine** How much memory would you like to use for this virtual machine? Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB. Memory for this virtual machine: 2048 MB Maximum recommended memory: 5952 MB Recommended memory: 2048 MB Guest OS recommended minimum: 1024 MB 64 GB 32 GB 16 GB 8 GB 4 GB 2 GB 1 GB 512 MB 256 MB 128 MB 64 MB 32 MB 16 MB 8 MB 4 MB Help < Back Next > Cancel
Step 11: In the **Network Type** window, leave the default selection.	 New Virtual Machine Wizard **Network Type** What type of network do you want to add? Network connection ○ Use bridged networking Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network. ● Use network address translation (NAT) Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address. ○ Use host-only networking Connect the guest operating system to a private virtual network on the host computer. ○ Do not use a network connection

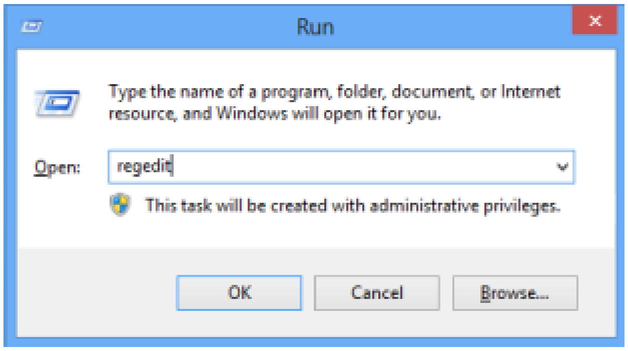
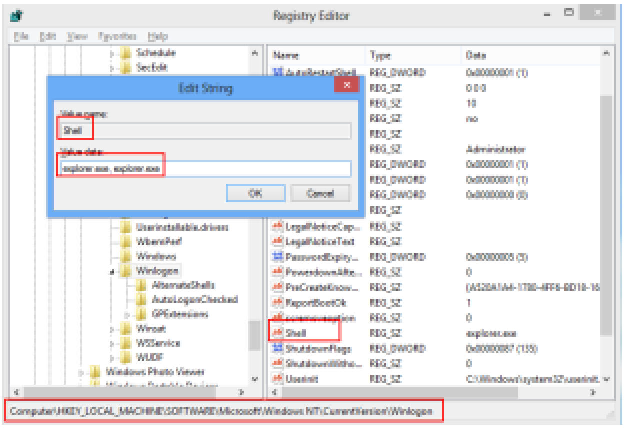
Step	Details
Step 12: In the **Select I/O Controller Types** , leave the default selection.	 New Virtual Machine Wizard **Select I/O Controller Types** Which SCSI controller type would you like to use? I/O controller types SCSI Controller: ○ BusLogic (Not available for 64-bit guests) ○ LSI Logic ● LSI Logic SAS (Recommended)
Step 13: In the **Select a Disk Type** page, select **IDE** and click **Next.** SCSI disks are not compatible with Advanced Threat Defense.	 New Virtual Machine Wizard **Select a Disk Type** What kind of disk do you want to create? Virtual disk type ● IDE ○ SCSI (Recommended) ○ SATA (Not supported on Workstation 9.0 VMs)

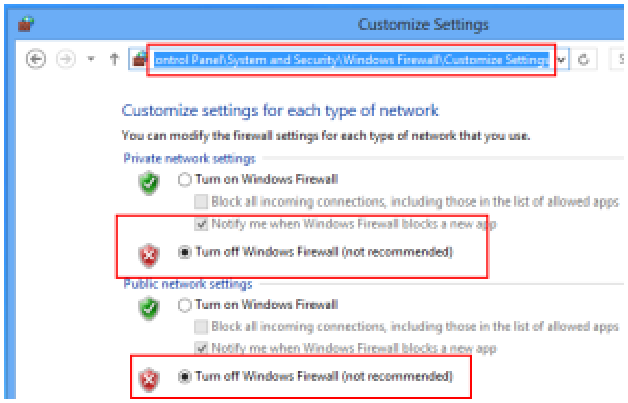
Step	Details
Step 14: In the **Select a Disk** window, select **Create a new virtual disk** and click **Next.**	 New Virtual Machine Wizard **Select a Disk** Which disk do you want to use? Disk ● Create a new virtual disk A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts. ○ Use an existing virtual disk Choose this option to reuse a previously configured disk. ○ Use a physical disk (for advanced users) Choose this option to give the virtual machine direct access to a local hard disk.
Step 15: Specify the details in the **Specify Disk Capacity** window and then click **Next.**	• **Maximum disk size (GB)** — For Windows 8 64-bit and 32-bit, the disk size can be 30 GB, however you must enter 24 GB for optimal performance. • Select **Allocate all disk space now.** • Select **Store virtual disk as a single file.**  New Virtual Machine Wizard **Specify Disk Capacity** How large do you want this disk to be? Maximum disk size (GB): 24 Recommended size for Windows 8 x64: 60 GB ☑ Allocate all disk space now. Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it. ● Store virtual disk as a single file ○ Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

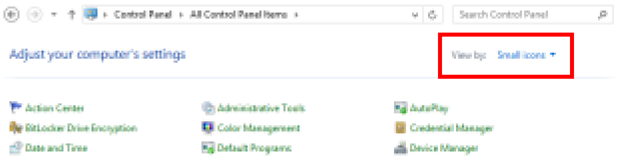
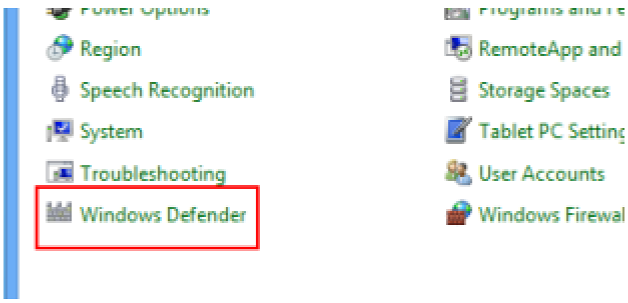
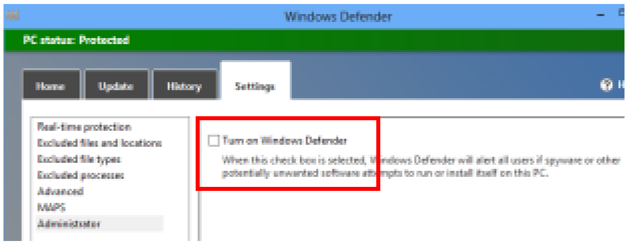
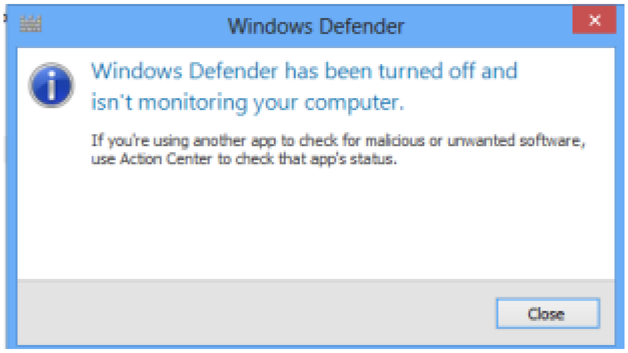
Step	Details
Step 16: In the **Specify Disk file** window, make sure virtualMachineImage.vmdk is displayed by default and click **Next**. If you specified a different name for **Virtual Machine name**, that name is displayed here.	 New Virtual Machine Wizard **Specify Disk File** Where would you like to store the disk file? Disk File One 24 GB disk file will be created using the file name provided here. virtualMachineImage.vmdk

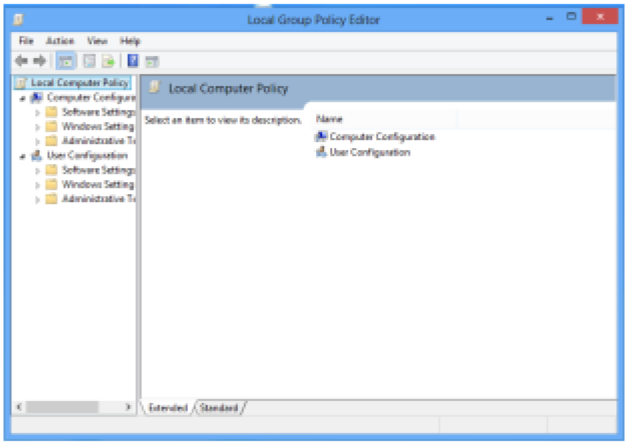
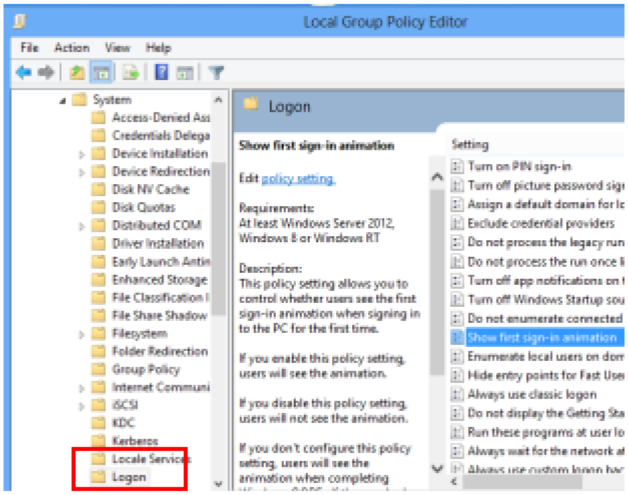
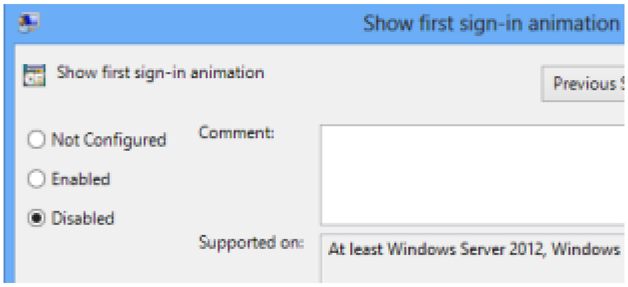
Step	Details
Step 17: Complete the following in the **Ready to Create Virtual Machine** window.	• **Power on this virtual machine after creation** — Select this option. • Click **Finish**. This step might take around 30 minutes to complete.  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows 8 x64 and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage Location: C:\01_[redacted]MATD_3.2.0\Win8 Version: Workstation 9.0 Operating System: Windows 8 x64 Hard Disk: 24 GB, Pre-allocated Memory: 2048 MB Network Adapter: NAT Other Devices: CD/DVD, USB Controller, Printer, Sound Card ☑ Power on this virtual machine after creation  New Virtual Machine Wizard **Ready to Create Virtual Machine** Click Finish to create the virtual machine and start installing Windows 8 x64 and then VMware Tools. The virtual machine will be created with the following settings: Name: virtualMachineImage VMware Workstation Creating Disk... ☑ Power on this virtual machine after creation Cancel Customize Hardware... < Back Finish Cancel

Step	Details
Step 18: If the **Removable Devices** pop-up window is displayed, select **Do not show this hint again** and click **OK**.	Windows begins to install, which might take around 15 minutes.  Installing Windows Your computer will restart several times. This might take a while. ✓ Copying Windows files **Getting files ready for installation (27%)** Installing features Installing updates Finishing up
Step 19: Log on to virtualMachineImage using the following credentials: • Administrator • cr@cker42	
Step 20: The VM by default displays in the Metro UI mode. Click the Desktop tile to switch to Desktop mode.	

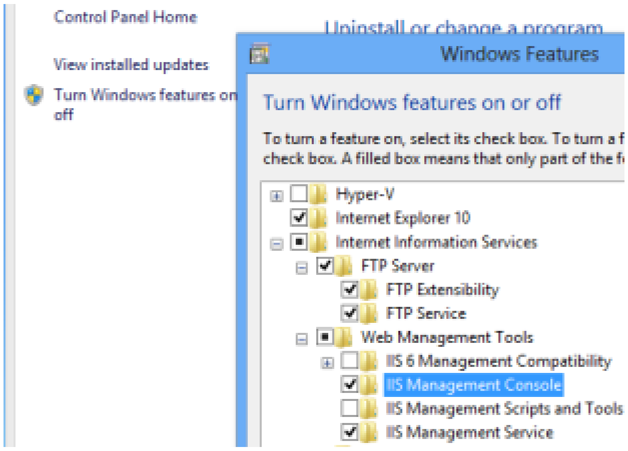
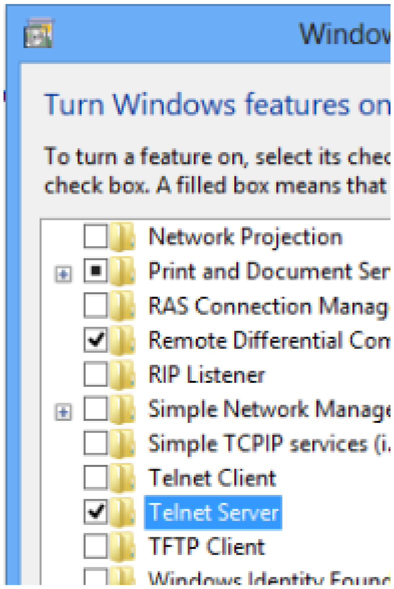
Step	Details
Step 21: Set up Windows 8 to display in the Desktop mode instead of the default Metro UI mode when it starts.	1 Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box. 2 In the **Run** dialog box, enter `regedit` and press Enter.  Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: regedit This task will be created with administrative privileges. The **Registry Editor** opens. 3 Select **HKEY_LOCAL_MACHINE | SOFTWARE | Microsoft | Windows NT | CurrentVersion | Winlogon** and then double-click on **Shell.** 4 Change **Value data** to `explorer.exe, explorer.exe` instead of the default value of `explorer.exe` and click **OK.**  Registry Editor Edit String Value name: Shell Value data: explorer.exe, explorer.exe Shell REG_SZ explorer.exe Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

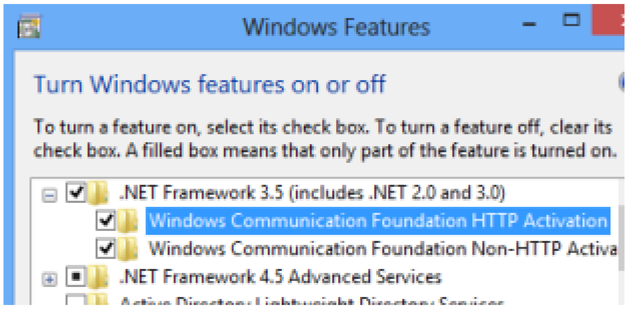
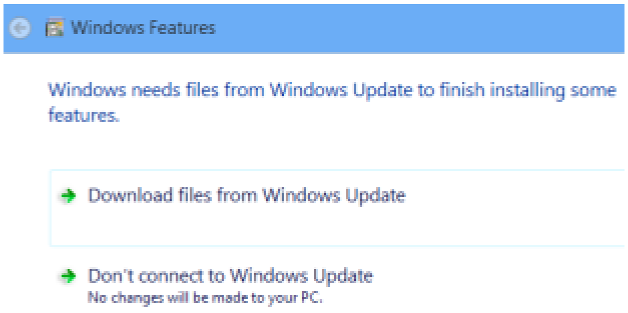
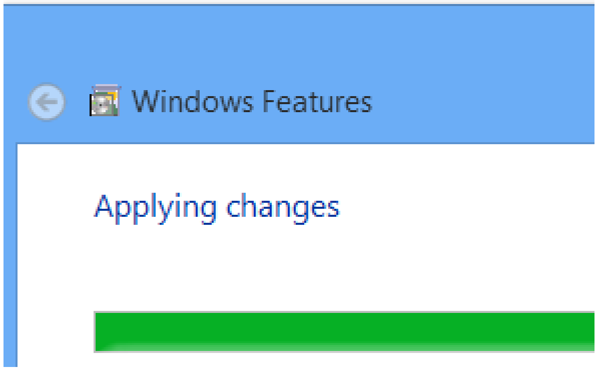
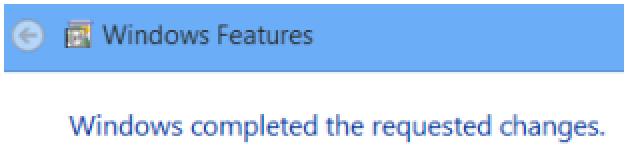
Step	Details
Step 22: In the VM, turn off the Windows Firewall.	1 Press the Windows key and X simultaneously and then select **Control Panel | System and Security | Windows Firewall | Turn on Windows Firewall On or Off**. 2 Select **Turn off Windows Firewall (not recommended)** for both **Home or work(private) network location settings** and **Public network location settings** and then click **OK**.  Customize Settings ontrol Panel\System and Security\Windows Firewall\Customize Settings Customize settings for each type of network You can modify the firewall settings for each type of network that you use. Private network settings ○ Turn on Windows Firewall □ Block all incoming connections, including those in the list of allowed apps ☑ Notify me when Windows Firewall blocks a new app ● Turn off Windows Firewall (not recommended) Public network settings ○ Turn on Windows Firewall □ Block all incoming connections, including those in the list of allowed apps ☑ Notify me when Windows Firewall blocks a new app ● Turn off Windows Firewall (not recommended)

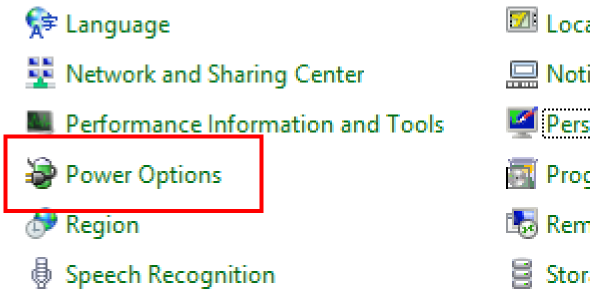
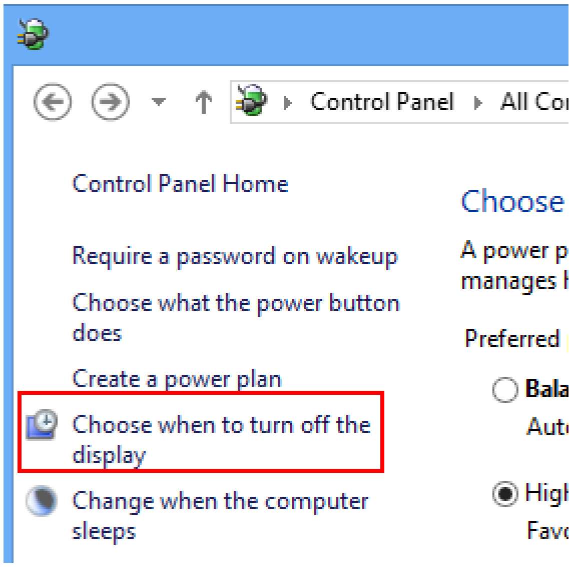
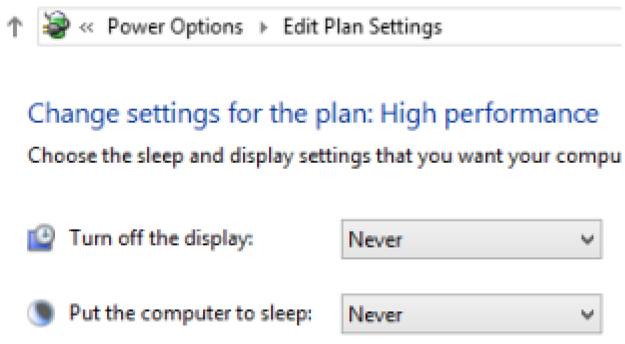
Step	Details
Step 23: Disable Windows Defender.	**1** Open the Control Panel and from the **View by** drop-down select **Small Icons.**  Control Panel › All Control Panel Items › Search Control Panel Adjust your computer's settings View by: Small icons ▾ Action Center BitLocker Drive Encryption Date and Time Administrative Tools Color Management Default Programs AutoPlay Credential Manager Device Manager **2** Click **Windows Defender.**  Power Options Region Speech Recognition System Troubleshooting Windows Defender Programs and F RemoteApp and Storage Spaces Tablet PC Setting User Accounts Windows Firewal **3** In **Windows Defender**, select **Settings** | **Administrators** and deselect **Turn on Windows Defender.** Then click **Save changes.**  Windows Defender PC status: Protected Home Update History Settings Real-time protection Excluded files and locations Excluded file types Excluded processes Advanced MAPS Administrator □ Turn on Windows Defender When this check box is selected, Windows Defender will alert all users if spyware or other potentially unwanted software attempts to run or install itself on this PC. **4** Close the Windows Defender message box.  Windows Defender has been turned off and isn't monitoring your computer. If you're using another app to check for malicious or unwanted software, use Action Center to check that app's status.

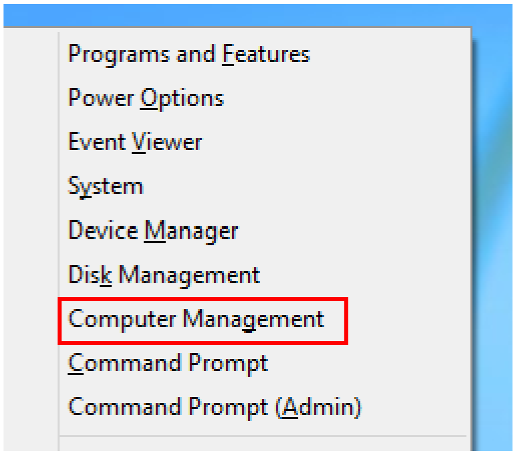
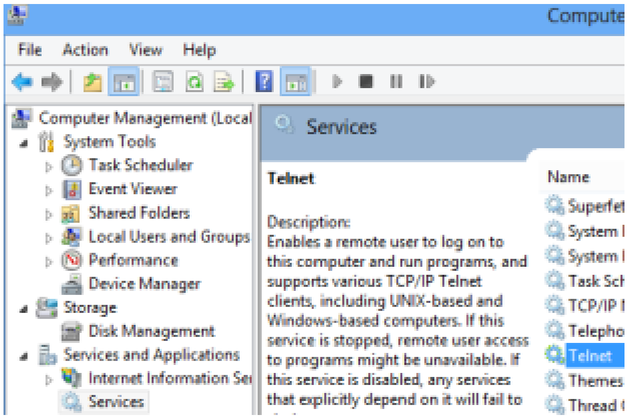
Step	Details
Step 24: Disable first sign-in animation.	1 Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box. 2 In the **Run** dialog box, enter `gpedit.msc` and press Enter. The **Local Group Policy Editor** opens.  Local Group Policy Editor File Action View Help Local Computer Policy Computer Configura Software Settings Windows Setting Administrative Te User Configuration Software Settings Windows Setting Administrative Te Local Computer Policy Select an item to view its description. Name Computer Configuration User Configuration Extended Standard 3 Select **Computer Configuration** | **Administrative Templates** | **System** | **Logon** and then open **Show first sign-in animation.**  Local Group Policy Editor File Action View Help System Access-Denied Ass Credentials Delega Device Installation Device Redirection Disk NV Cache Disk Quotas Distributed COM Driver Installation Early Launch Antim Enhanced Storage File Classification I File Share Shadow Filesystem Folder Redirection Group Policy Internet Communi iSCSI KDC Kerberos Locale Services Logon Logon Setting Turn on PIN sign-in Turn off picture password sig Assign a default domain for lo Exclude credential providers Do not process the legacy run Do not process the run once li Turn off app notifications on t Turn off Windows Startup sou Do not enumerate connected Show first sign-in animation Enumerate local users on dom Hide entry points for Fast Use Always use classic logon Do not display the Getting Sta Run these programs at user lo Always wait for the network at Always use custom logon bac Show first sign-in animation Edit policy setting. Requirements: At least Windows Server 2012, Windows 8 or Windows RT Description: This policy setting allows you to control whether users see the first sign-in animation when signing in to the PC for the first time. If you enable this policy setting, users will see the animation. If you disable this policy setting, users will not see the animation. If you don't configure this policy setting, users will see the animation when completing 4 Select **Disabled** and then click **OK**.  Show first sign-in animation Show first sign-in animation Previous S Comment: Supported on: ○ Not Configured ○ Enabled ● Disabled Supported on: At least Windows Server 2012, Windows

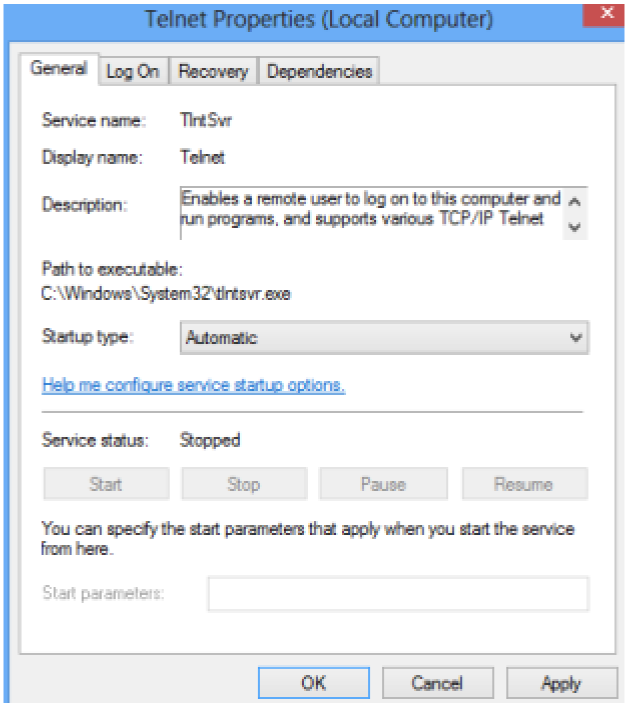
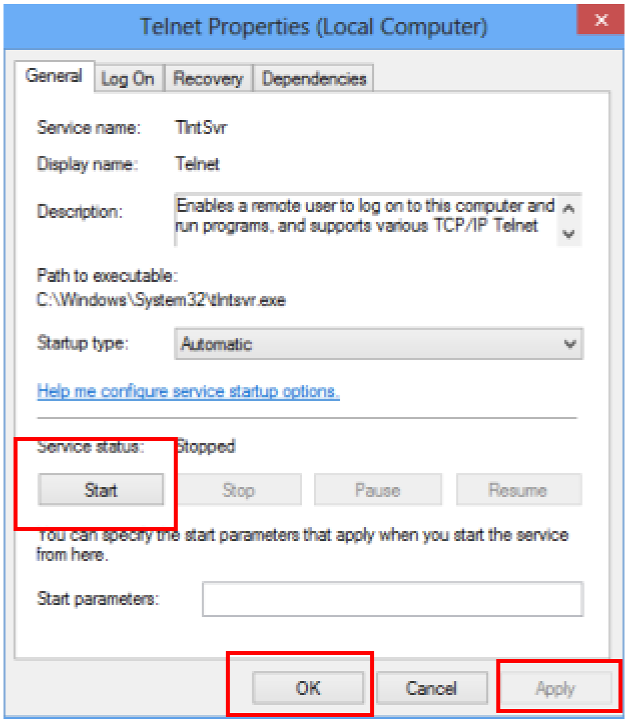
Step	Details

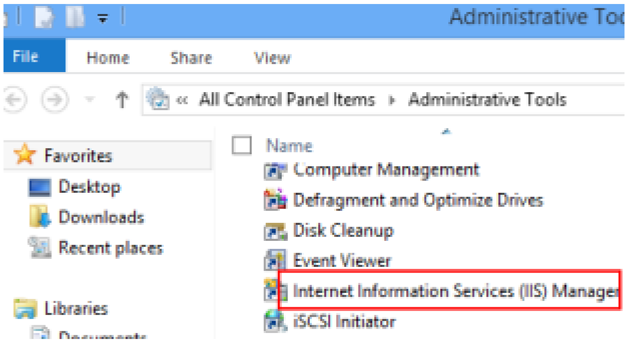
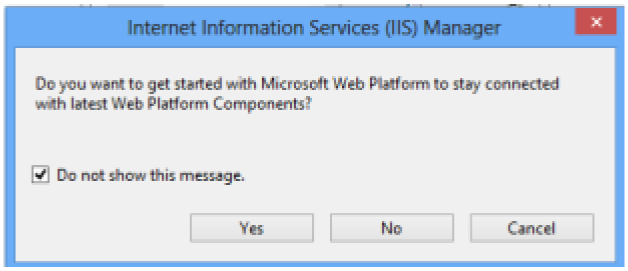
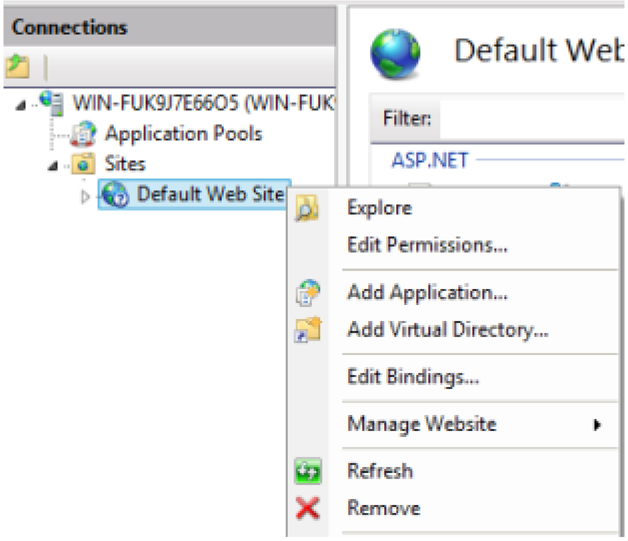
Step	Details
Step 25: Press the Windows key and X simultaneously and then select **Control Panel** | **Programs** | **Programs and Features** | **Turn Windows feature on or off** and complete the following.	1 Select **Internet Information Services** | **FTP server** and select **FTP Extensibility**. 2 Select **Internet Information Services** | **Web Management Tools** and select **IIS Management Console** and **IIS Management Service**.  Control Panel Home View installed updates Turn Windows features on or off Uninstall or change a program Windows Features Turn Windows features on or off To turn a feature on, select its check box. To turn a f check box. A filled box means that only part of the f ⊞ □ Hyper-V ☑ Internet Explorer 10 ⊟ ■ Internet Information Services ⊟ ☑ FTP Server ☑ FTP Extensibility ☑ FTP Service ⊟ ■ Web Management Tools ⊞ □ IIS 6 Management Compatibility ☑ IIS Management Console □ IIS Management Scripts and Tools ☑ IIS Management Service 3 Select **Telnet Server.**  Windov Turn Windows features on To turn a feature on, select its chec check box. A filled box means that □ Network Projection ⊞ ■ Print and Document Ser □ RAS Connection Manag ☑ Remote Differential Con □ RIP Listener ⊞ □ Simple Network Manage □ Simple TCPIP services (i. □ Telnet Client ☑ Telnet Server □ TFTP Client □ Windows Identity Founc 4 Select **.NET Framework 3.5(includes .NET 2.0 and3.0)** and then select **Windows Communication Foundation HTTP Activation** and **Windows Communication Foundation Non-HTP Activation** options.

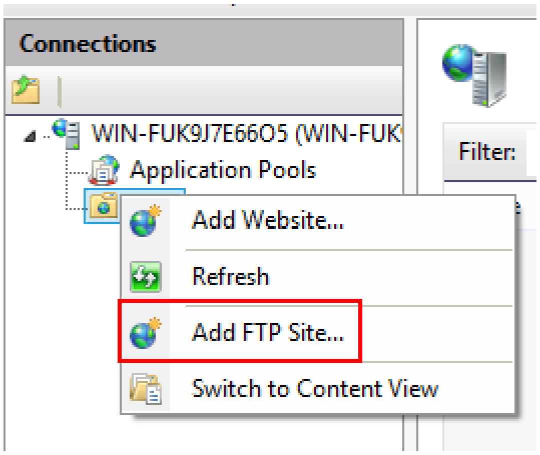
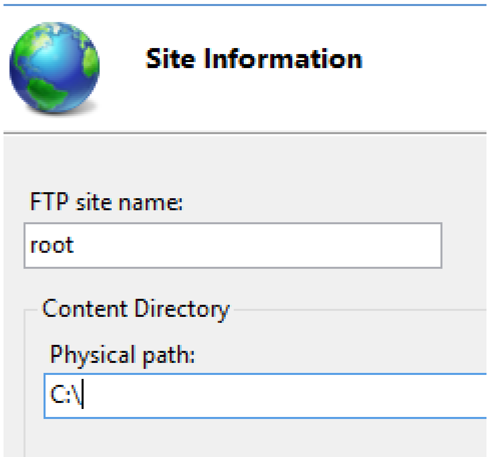
Step	Details
	 Windows Features Turn Windows features on or off To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on. ☑ .NET Framework 3.5 (includes .NET 2.0 and 3.0) ☑ Windows Communication Foundation HTTP Activation ☑ Windows Communication Foundation Non-HTTP Activa ■ .NET Framework 4.5 Advanced Services **5** Press **OK**. **6** If the following message is displayed, select **Download files from Windows Update.**  Windows Features Windows needs files from Windows Update to finish installing some features. Download files from Windows Update Don't connect to Windows Update No changes will be made to your PC. This operation might take around 5 minutes to complete.  Windows Features Applying changes A confirmation message is displayed when the operation completes.  Windows Features Windows completed the requested changes.

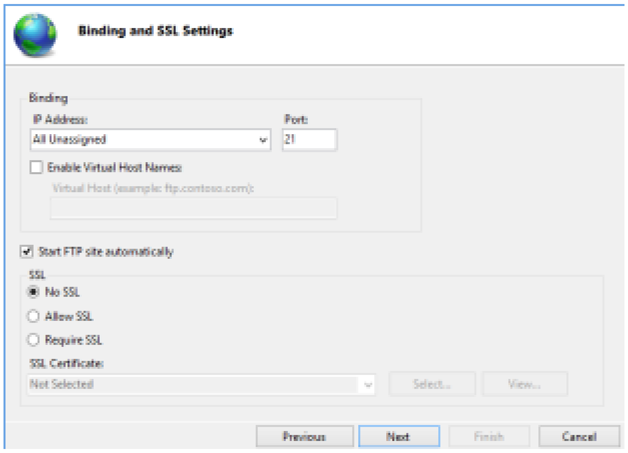
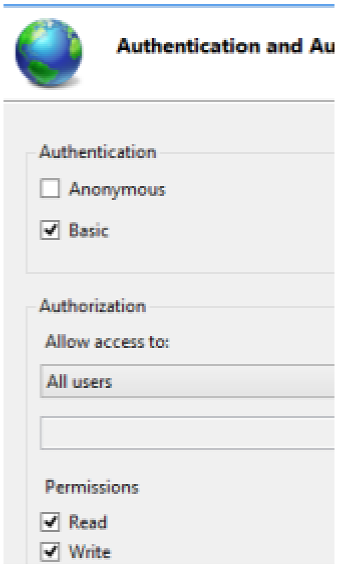
Step	Details
Step 26: Edit the power options.	1 Open the Control Panel and from the **View by** drop-down select **Small Icons.** 2 Click **Power Options.**  Language Network and Sharing Center Performance Information and Tools Power Options Region Speech Recognition Loca Noti Pers Prog Rem Stor 3 Click **Choose when to turn off the display.**  Control Panel All Co Control Panel Home Require a password on wakeup Choose what the power button does Create a power plan Choose when to turn off the display Change when the computer sleeps Choose A power p manages Preferred ○ Bala Aut ● High Fav 4 Select **Never** for **Turn off the display** and **Put the computer to sleep** and then click **Save changes.**  Change settings for the plan: High performance Choose the sleep and display settings that you want your compu Turn off the display: Never Put the computer to sleep: Never

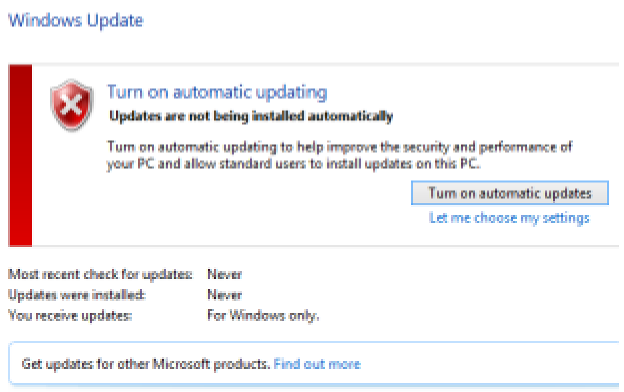
Step	Details
Step 27: Press the Windows key and X simultaneously and then select **Computer Management** | **Services and Applications** | **Services.** Then double-click on **Telnet.**	 Programs and Features Power Options Event Viewer System Device Manager Disk Management Computer Management Command Prompt Command Prompt (Admin)  Compute File Action View Help Computer Management (Local System Tools Task Scheduler Event Viewer Shared Folders Local Users and Groups Performance Device Manager Storage Disk Management Services and Applications Internet Information Se Services Services Name Superfet System I System I Task Sch TCP/IP I Telepho Telnet Themes Thread (**Telnet** Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet clients, including UNIX-based and Windows-based computers. If this service is stopped, remote user access to programs might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to

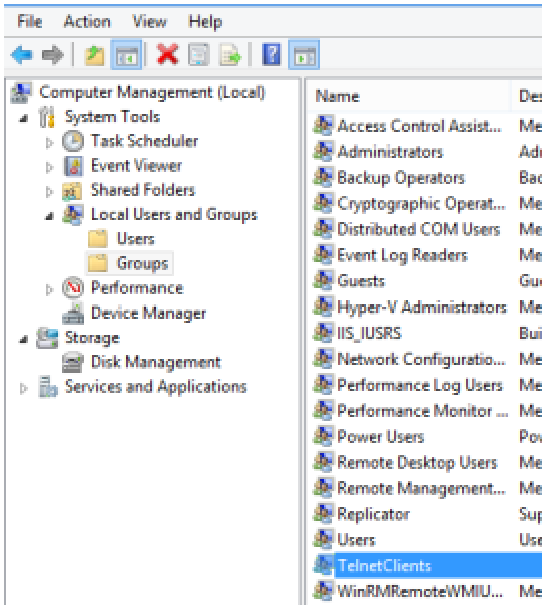
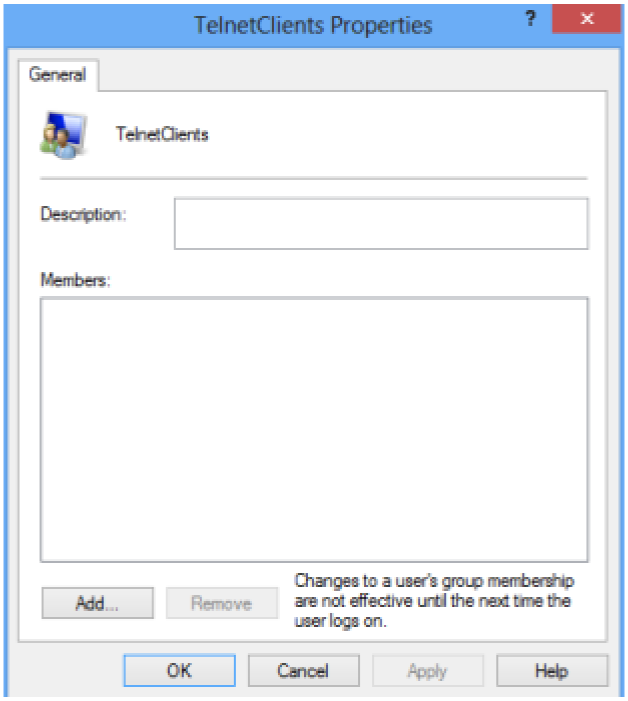
Step	Details
Step 28: In the Telnet Properties (Local Computer) dialog, select **Automatic** from the **Startup type** list. Then select **Apply** | **Start** | **OK**.	 Telnet Properties (Local Computer) General Log On Recovery Dependencies Service name: TlntSvr Display name: Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet Path to executable: C:\Windows\System32\tlntsvr.exe Startup type: Automatic Help me configure service startup options. Service status: Stopped Start Stop Pause Resume You can specify the start parameters that apply when you start the service from here. Start parameters:  Telnet Properties (Local Computer) General Log On Recovery Dependencies Service name: TlntSvr Display name: Telnet Description: Enables a remote user to log on to this computer and run programs, and supports various TCP/IP Telnet Path to executable: C:\Windows\System32\tlntsvr.exe Startup type: Automatic Help me configure service startup options. Service status: Stopped Start Stop Pause Resume You can specify the start parameters that apply when you start the service from here. Start parameters:

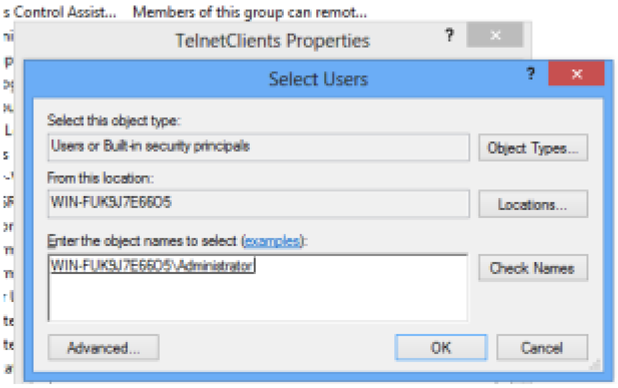
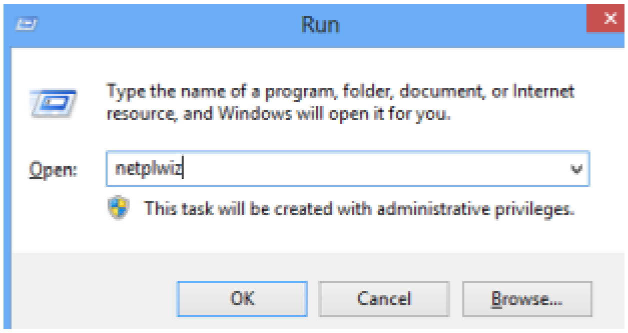
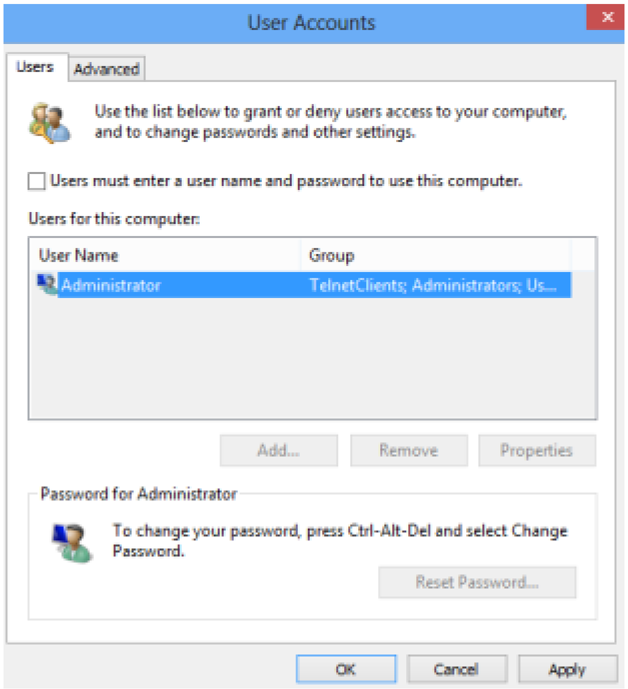
Step	Details
Step 29: Enable FTP on Windows 8.	1 Press the Windows key and X simultaneously and then select **Control Panel** | **System and Security** | **Administrative Tools**.  Administrative To File Home Share View « All Control Panel Items ▸ Administrative Tools Favorites Desktop Downloads Recent places Libraries Documents Name Computer Management Defragment and Optimize Drives Disk Cleanup Event Viewer Internet Information Services (IIS) Manager iSCSI Initiator 2 Double-click **Internet Information Services(IIS) Manager**, expand the tree under **Hostname**. 3 If you see the following message box, select **Do not show this message** and click **Cancel.** 4 Select **Site**  Internet Information Services (IIS) Manager Do you want to get started with Microsoft Web Platform to stay connected with latest Web Platform Components? ☑ Do not show this message. **s** and right-click **Default Web Site** and then select **Remove**. Confirm by clicking **Yes.**  Connections WIN-FUK9J7E66O5 (WIN-FUK Application Pools Sites Default Web Site Default Wet Filter: ASP.NET Explore Edit Permissions... Add Application... Add Virtual Directory... Edit Bindings... Manage Website Refresh Remove

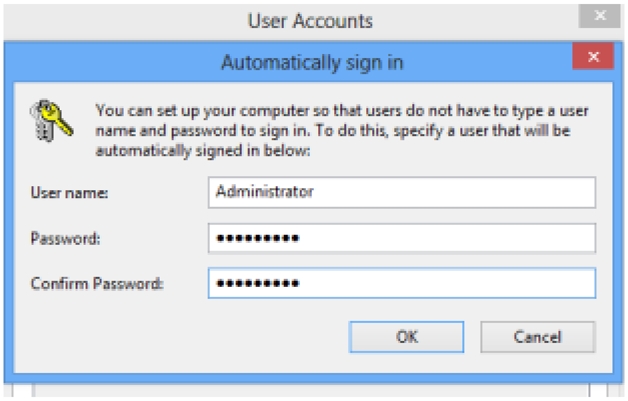
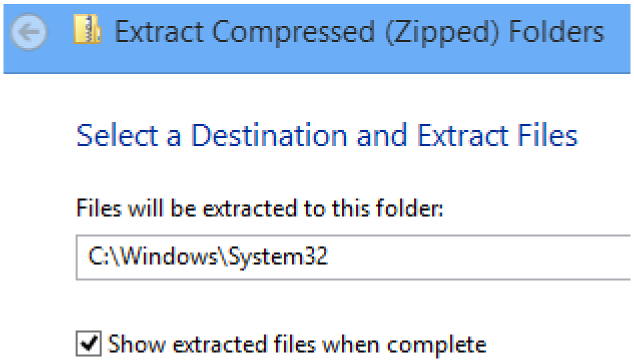
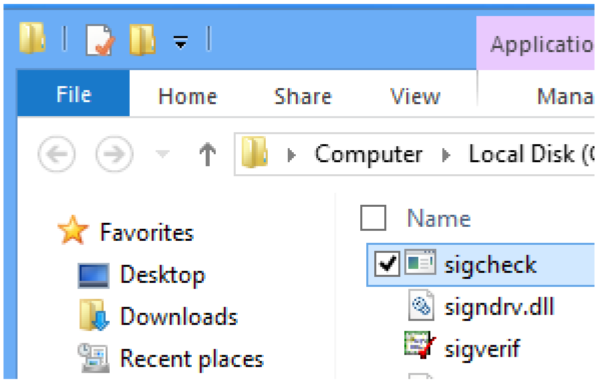
Step	Details
	5 Right-click **Sites** and select **Add FTP Site**. Then complete the following.  Connections WIN-FUK9J7E66O5 (WIN-FUK Application Pools Filter: Add Website... Refresh Add FTP Site... Switch to Content View a For **FTP site name**, enter `root`. b **Physical Path: C:\\.** c Click **Next**.  Site Information FTP site name: root Content Directory Physical path: C:\\ 6 For **Bindings and SSL Settings**, select **No SSL**. For all other fields, leave the default values and click **Next**.

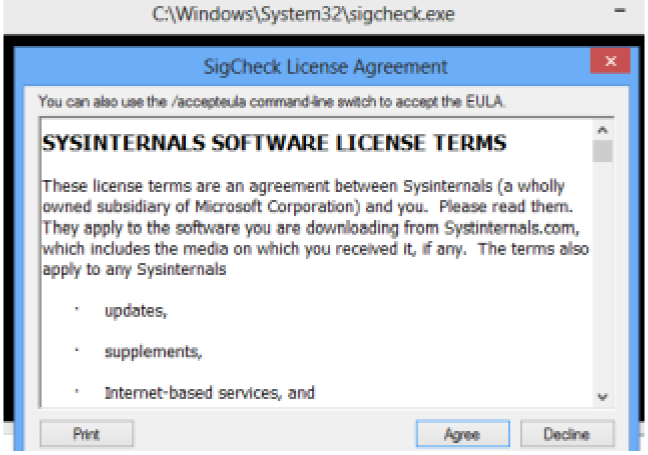
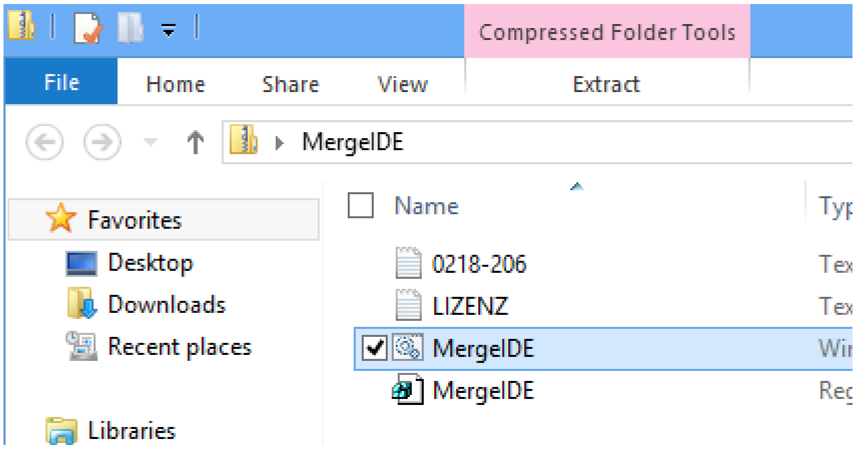
Step	Details
	 Binding and SSL Settings Binding IP Address: All Unassigned Port: 21 □ Enable Virtual Host Names Virtual Host (example: ftp.contoso.com): ☑ Start FTP site automatically SSL ● No SSL ○ Allow SSL ○ Require SSL SSL Certificate: Not Selected 7 For **Authentication and Authorization Information** complete the following. a Select **Basic**. b For **Allow access to**, select **All Users.** c For **Permissions**, select both **Read** and **Write**, and then click **Finish.** d Close the **Internet Information Services (IIS) Manager.**  Authentication and Au Authentication □ Anonymous ☑ Basic Authorization Allow access to: All users Permissions ☑ Read ☑ Write

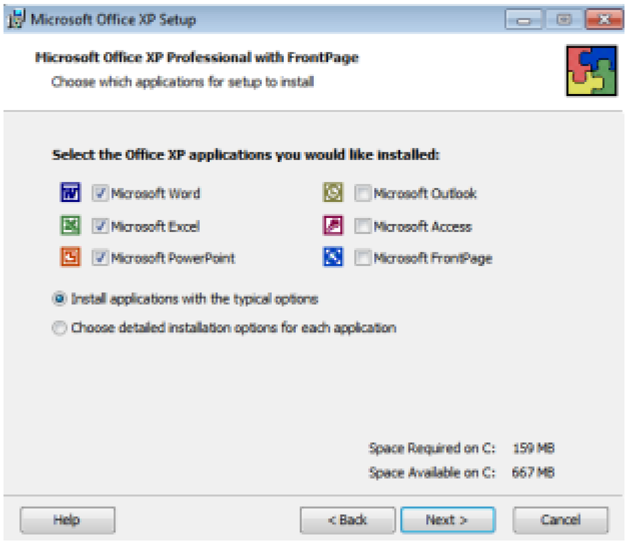
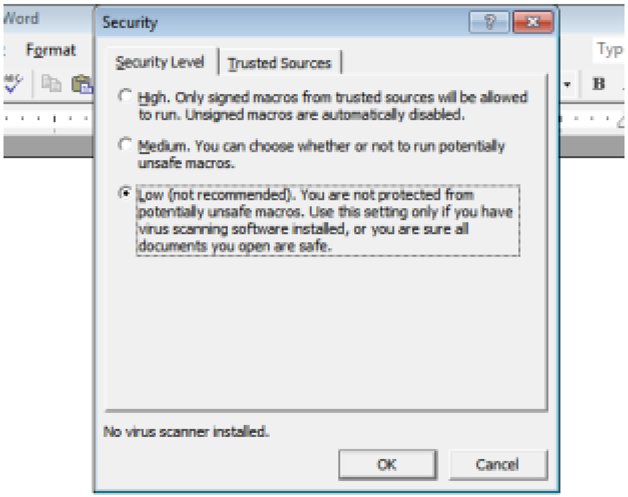
Step	Details
Step 30: Turn off automatic updating for Windows.	1 Press the Windows key and X simultaneously and then select **Control Panel | Windows Update | Change**. 2 Select **Never check for updates (not recommended)** and click **OK.**  Windows Update Turn on automatic updating **Updates are not being installed automatically** Turn on automatic updating to help improve the security and performance of your PC and allow standard users to install updates on this PC. Turn on automatic updates Let me choose my settings Most recent check for updates: Never Updates were installed: Never You receive updates: For Windows only. Get updates for other Microsoft products. Find out more

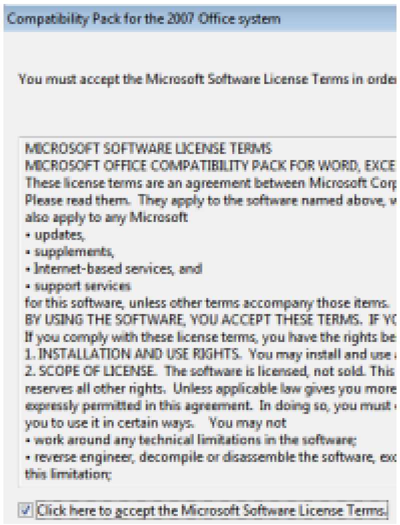
Step	Details
Step 31: Complete the following: 1 Open the Control Panel and from the **View by** drop-down select **Small Icons.** 2 Select **Administrator Tools** | **Computer Management** and complete the steps in the next column.	1 Select **Computer Management (Local)** | **System Tools** | **Local Users and Groups** | **Groups**  File Action View Help Computer Management (Local) System Tools Task Scheduler Event Viewer Shared Folders Local Users and Groups Users Groups Performance Device Manager Storage Disk Management Services and Applications Name Des Access Control Assist... Administrators Backup Operators Cryptographic Operat... Distributed COM Users Event Log Readers Guests Hyper-V Administrators IIS_IUSRS Network Configuratio... Performance Log Users Performance Monitor ... Power Users Remote Desktop Users Remote Management... Replicator Users TelnetClients WinRMRemoteWMIU... 2 Double-click **TelnetClients.**  TelnetClients Properties ? × General TelnetClients Description: Members: Add... Remove OK Cancel Apply Help Changes to a user's group membership are not effective until the next time the user logs on. 3 Click **Add** and enter `Administrator`. 4 Click **Check Names** and then **OK.**

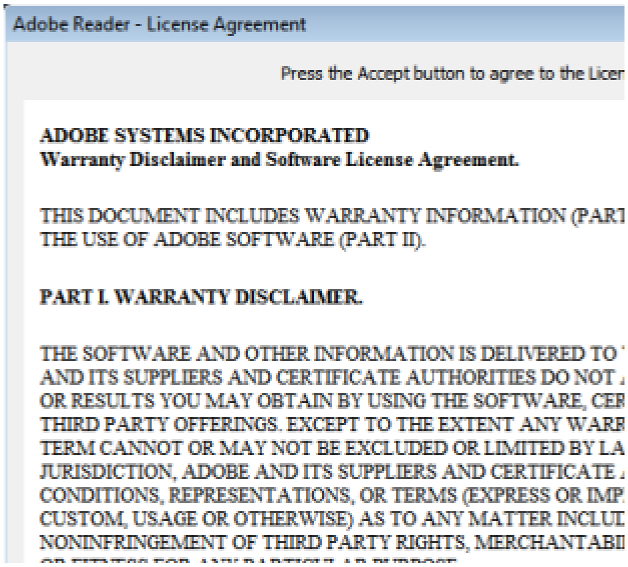
Step	Details
	 s Control Assist... Members of this group can remot... TelnetClients Properties Select Users Select this object type: Users or Built-in security principals Object Types... From this location: WIN-FUK5J7E66O5 Locations... Enter the object names to select (examples): WIN-FUK5J7E66O5\Administrator Check Names Advanced... OK Cancel
Step 32: Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box. Then enter `netplwiz` and click **OK**.	 Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: netplwiz This task will be created with administrative privileges. OK Cancel Browse...
Step 33: In the **User Accounts** window, deselect **Users must enter a user name and password to use this computer** and click **Apply.**	 User Accounts Users Advanced Use the list below to grant or deny users access to your computer, and to change passwords and other settings. □ Users must enter a user name and password to use this computer. Users for this computer: User Name: Administrator — Group: TelnetClients; Administrators; Us... Add... Remove Properties Password for Administrator To change your password, press Ctrl-Alt-Del and select Change Password. Reset Password... OK Cancel Apply

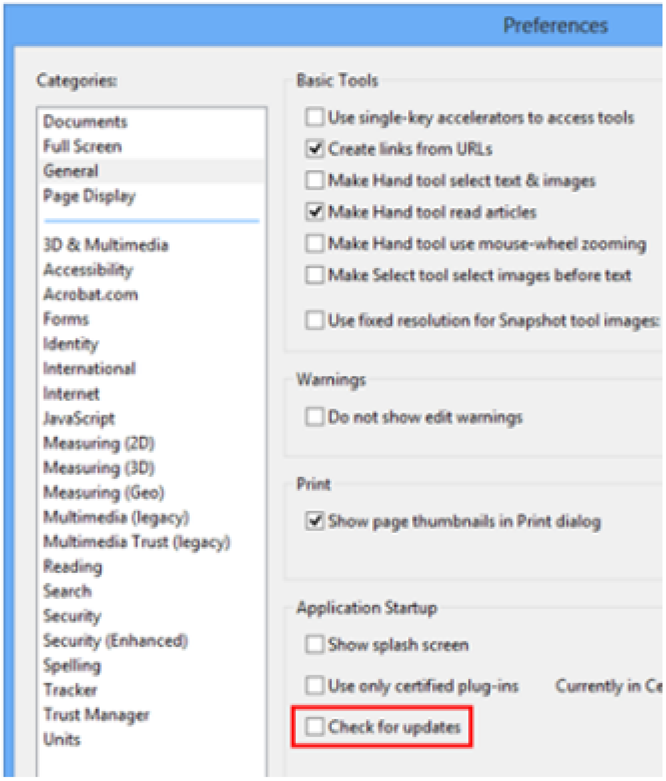
Step	Details
Step 34: In the **Automatically sign in** pop-up window, complete the following and then press **OK** in the message boxes.	• **User name** — Enter `Administrator` • **Password** — Enter `cr@cker42` • **Confirm Password** — Enter `cr@cker42`  User Accounts Automatically sign in You can set up your computer so that users do not have to type a user name and password to sign in. To do this, specify a user that will be automatically signed in below: User name: Administrator Password: •••••••••• Confirm Password: ••••••••••
Step 35: Download Sigcheck on to your computer (the native host) from http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx.	The VM that you created has the Windows Firewall switch off as well as there is no anti-virus installed on it. Therefore, it is recommended that you download the programs and components on to the native host first and then copy them to the VM in VMware Workstation.
Step 36: Extract sigcheck.zip to `C:\WINDOWS\system32` location.	 Extract Compressed (Zipped) Folders Select a Destination and Extract Files Files will be extracted to this folder: C:\Windows\System32 ☑ Show extracted files when complete
Step 37: In Windows Explorer, go to C:\WINDOWS\system32 and double-click **sigcheck.exe**.	 Applicatio File Home Share View Mana Computer Local Disk (Favorites Desktop Downloads Recent places Name sigcheck signdrv.dll sigverif

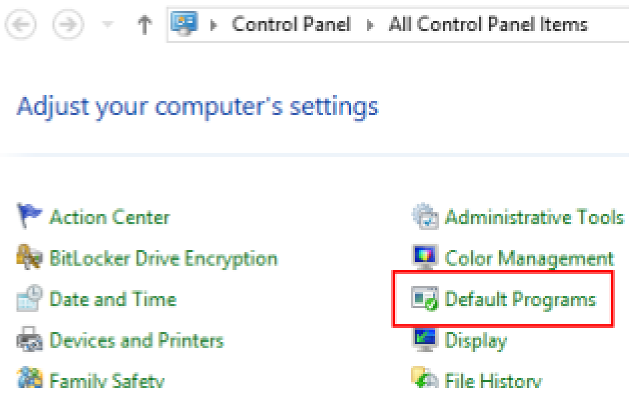
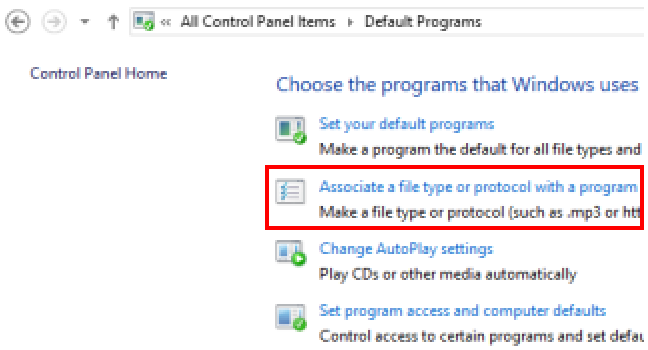
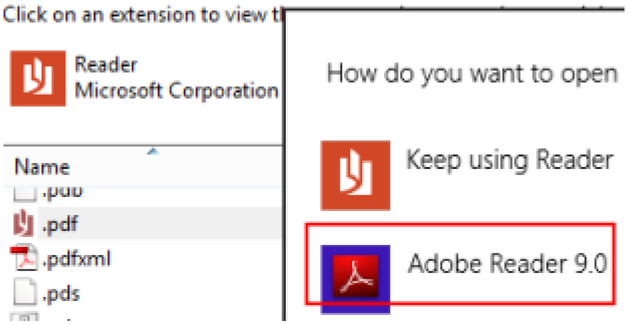
Step	Details
Step 38: Click **Agree** for **Sigcheck License Agreement.** After you click on **Agree**, no confirmation message is displayed.	 C:\Windows\System32\sigcheck.exe SigCheck License Agreement Print Agree Decline You can also use the /accepteula command-line switch to accept the EULA. **SYSINTERNALS SOFTWARE LICENSE TERMS** These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals · updates, · supplements, · Internet-based services, and
Step 39: Download MergeIDE.zip from https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip on to the native computer and then copy it to the VM.	
Step 40: Extract MergeIDE.zip and run the MergeIDE batch file in the VM.	 Compressed Folder Tools File Home Share View Extract MergeIDE Favorites Desktop Downloads Recent places Libraries Name Typ 0218-206 Tex LIZENZ Tex MergeIDE Wir MergeIDE Reg • If prompted, select **Run** in the warning message. • Close Windows Explorer.

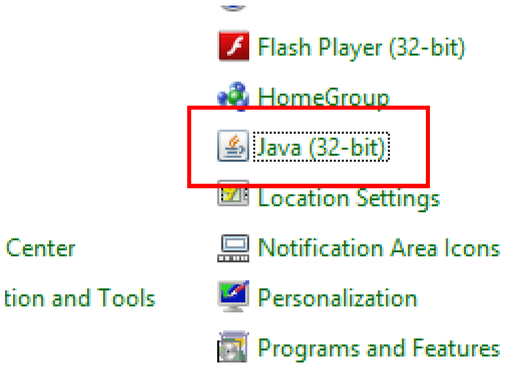
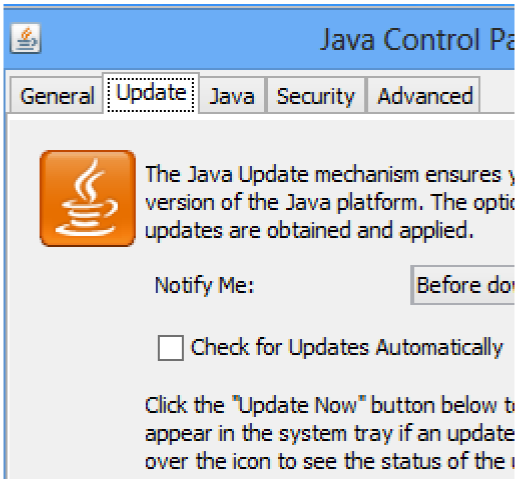
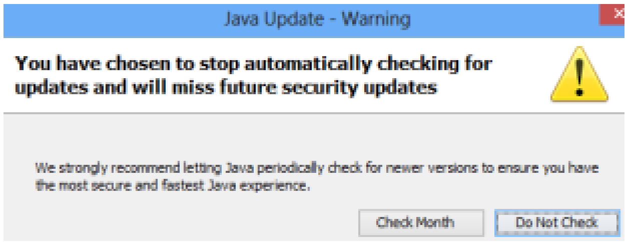
Step	Details
Step 41: To analyze Microsoft Word, Excel, and Powerpoint files, install Microsoft Office 2003 on the virtual machine.	 Microsoft Office XP Setup **Microsoft Office XP Professional with FrontPage** Choose which applications for setup to install **Select the Office XP applications you would like installed:** ☑ Microsoft Word ☐ Microsoft Outlook ☑ Microsoft Excel ☐ Microsoft Access ☑ Microsoft PowerPoint ☐ Microsoft FrontPage ● Install applications with the typical options ○ Choose detailed installation options for each application Space Required on C: 159 MB Space Available on C: 667 MB
Step 42: Lower the security to run macros for the Office applications.	• Open Microsoft Word 2003 and select **Tools** | **Macro** | **Security** and then select **Low** and click **OK**.  Security Security Level | Trusted Sources ○ High. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled. ○ Medium. You can choose whether or not to run potentially unsafe macros. ● Low (not recommended). You are not protected from potentially unsafe macros. Use this setting only if you have virus scanning software installed, or you are sure all documents you open are safe. No virus scanner installed. • Similarly lower the macro security for Microsoft Excel and PowerPoint.

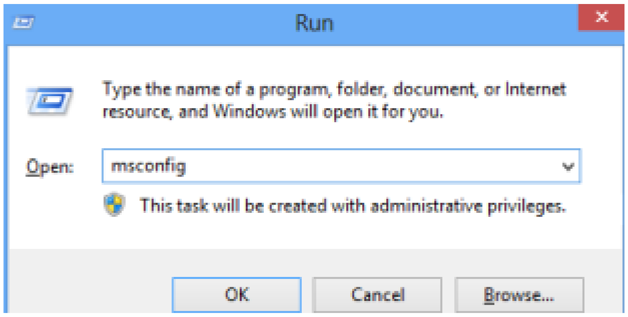
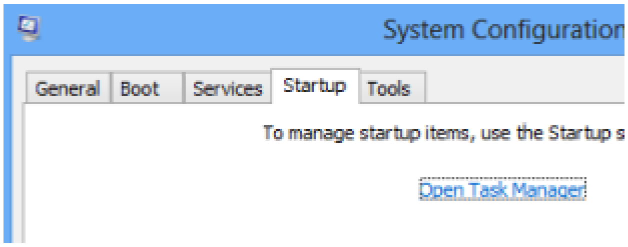
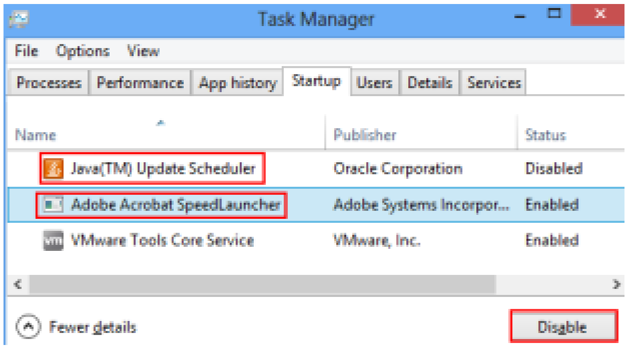
Step	Details
Step 43: You need the compatibility pack to open Microsoft Office files that were created in a newer version of Microsoft Office. For example, to open a .docx file using Office 2003, you need the corresponding compatibility pack installed. Go to http://www.microsoft.com/en-us/download/details.aspx?id=3 and download the required Microsoft Office compatibility pack for Word, Excel, and PowerPoint File Formats. Then install them on the virtual machine.	In the **Compatibility Pack for the 2007 Office system** dialog, select **Click here to accept the Microsoft Software License Terms** and click **Continue.**  Compatibility Pack for the 2007 Office system You must accept the Microsoft Software License Terms in orde MICROSOFT SOFTWARE LICENSE TERMS MICROSOFT OFFICE COMPATIBILITY PACK FOR WORD, EXCE These license terms are an agreement between Microsoft Corp Please read them. They apply to the software named above, w also apply to any Microsoft • updates, • supplements, • Internet-based services, and • support services for this software, unless other terms accompany those items. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YO If you comply with these license terms, you have the rights be 1. INSTALLATION AND USE RIGHTS. You may install and use a 2. SCOPE OF LICENSE. The software is licensed, not sold. This reserves all other rights. Unless applicable law gives you more expressly permitted in this agreement. In doing so, you must you to use it in certain ways. You may not • work around any technical limitations in the software; • reverse engineer, decompile or disassemble the software, exc this limitation; ☑ Click here to accept the Microsoft Software License Terms.

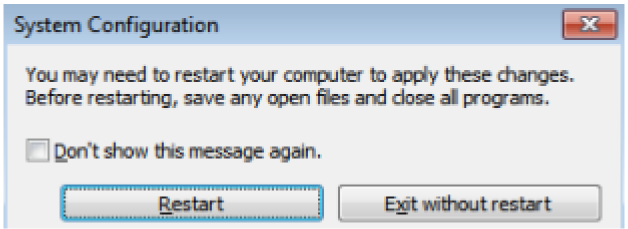
Step	Details
Step 44: To analyze PDF files, download Adobe Reader to the native host and copy it to the VM. This procedure uses Adobe Reader 9.0 as an example.	1 Install Adobe Reader 9.0 in the VM. 2 Open Adobe Reader and click **Accept**.  Adobe Reader - License Agreement Press the Accept button to agree to the Licen **ADOBE SYSTEMS INCORPORATED** **Warranty Disclaimer and Software License Agreement.** THIS DOCUMENT INCLUDES WARRANTY INFORMATION (PART THE USE OF ADOBE SOFTWARE (PART II). **PART I. WARRANTY DISCLAIMER.** THE SOFTWARE AND OTHER INFORMATION IS DELIVERED TO AND ITS SUPPLIERS AND CERTIFICATE AUTHORITIES DO NOT OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE, CER THIRD PARTY OFFERINGS. EXCEPT TO THE EXTENT ANY WARR TERM CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LA JURISDICTION, ADOBE AND ITS SUPPLIERS AND CERTIFICATE CONDITIONS, REPRESENTATIONS, OR TERMS (EXPRESS OR IMP CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUD NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABI

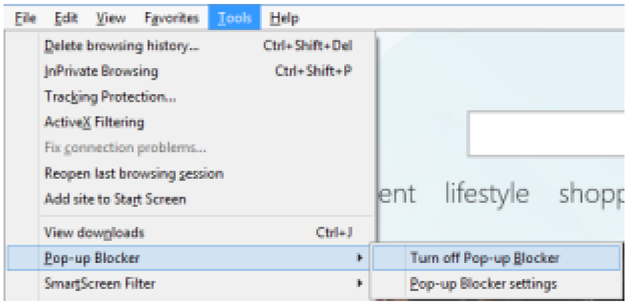
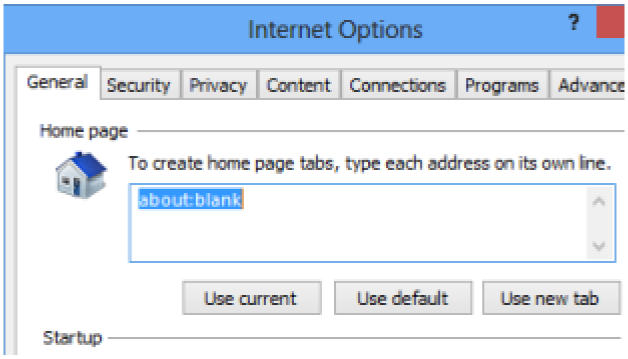
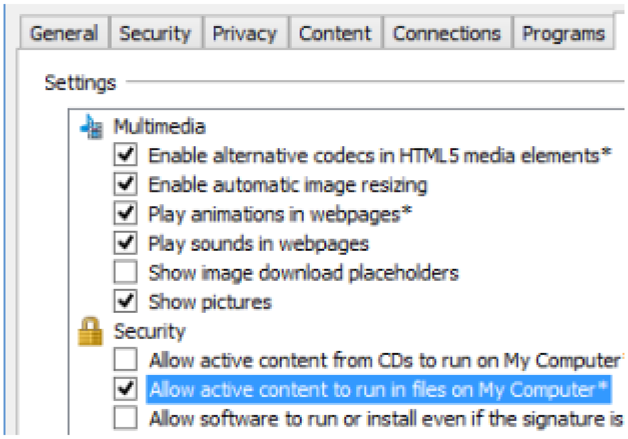
Step	Details
	3 a In Adobe Reader, select **Edit** | **Preferences** | **General** and deselect **Check for updates.** b In Adobe Reader, select **Help** | **Check for updates** | **Preferences** and deselect **Adobe Updates.**  Preferences Categories: Documents Full Screen General Page Display 3D & Multimedia Accessibility Acrobat.com Forms Identity International Internet JavaScript Measuring (2D) Measuring (3D) Measuring (Geo) Multimedia (legacy) Multimedia Trust (legacy) Reading Search Security Security (Enhanced) Spelling Tracker Trust Manager Units Basic Tools □ Use single-key accelerators to access tools ☑ Create links from URLs □ Make Hand tool select text & images ☑ Make Hand tool read articles □ Make Hand tool use mouse-wheel zooming □ Make Select tool select images before text □ Use fixed resolution for Snapshot tool images: Warnings □ Do not show edit warnings Print ☑ Show page thumbnails in Print dialog Application Startup □ Show splash screen □ Use only certified plug-ins Currently in Ce □ Check for updates

Step	Details
Step 45: Set Adobe Reader 9 as the default application to open PDF files.	1 In the **Control Panel** (icons view), select **Default Programs.**  Control Panel › All Control Panel Items Adjust your computer's settings Action Center Administrative Tools BitLocker Drive Encryption Color Management Date and Time Default Programs Devices and Printers Display Family Safety File History 2 Select **Associate a file type or protocol with a program**  « All Control Panel Items › Default Programs Control Panel Home Choose the programs that Windows uses Set your default programs Make a program the default for all file types and Associate a file type or protocol with a program Make a file type or protocol (such as .mp3 or htt Change AutoPlay settings Play CDs or other media automatically Set program access and computer defaults Control access to certain programs and set defau 3 Locate **.pdf** and double click on it. Chose Adobe Reader 9.0 as the default PDF reader.  Click on an extension to view t Reader Microsoft Corporation Name .pub .pdf .pdfxml .pds How do you want to open Keep using Reader Adobe Reader 9.0
Step 46: To analyze JAR files, download and install Java Runtime Environment.	1 Goto https://community.mcafee.com/docs/DOC-6858. 2 Refer **Java installation guidance.docx.**

Step	Details
Step 47: Open Java in Control Panel.	 Flash Player (32-bit) HomeGroup Java (32-bit) Location Settings Center Notification Area Icons tion and Tools Personalization Programs and Features
Step 48: In the **Update** tab, deselect **Check for Updates Automatically.**	 Java Control Pa General Update Java Security Advanced The Java Update mechanism ensures y version of the Java platform. The optic updates are obtained and applied. Notify Me: Before do □ Check for Updates Automatically Click the "Update Now" button below t appear in the system tray if an update over the icon to see the status of the u
Step 49: In the Java Update Warning dialog, select **Do Not Check** and then click **OK** in the Java Control Panel.	 Java Update - Warning **You have chosen to stop automatically checking for updates and will miss future security updates** We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.

Step	Details
Step 50: Disable *jusched* and *reader_sl*.	1 Press the Windows key and R simultaneously, which is the shortcut to open the **Run** dialog box. In the Windows Run dialog, enter `msconfig` and click **OK**.  Run Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. Open: msconfig This task will be created with administrative privileges. 2 In the **System Configuration** utility, go to the **Startup** tab.  System Configuration To manage startup items, use the Startup s 3 Click **Open Task Manager.** 4 If *Java(TM) Update Scheduler* (jusched) is listed, select it and click **Disable.** 5 If *Adobe Acrobat SpeedLauncher* (reader_sl) is listed, select it and click **Disable.**  Task Manager File Options View Processes Performance App history Startup Users Details Services Name — Publisher — Status Java(TM) Update Scheduler — Oracle Corporation — Disabled Adobe Acrobat SpeedLauncher — Adobe Systems Incorpor... — Enabled VMware Tools Core Service — VMware, Inc. — Enabled 6 In the **System Configuration** dialog, select **Don't show this message again** and click **Restart.**

Step	Details
	 System Configuration You may need to restart your computer to apply these changes. Before restarting, save any open files and close all programs. □ Don't show this message again.

Step	Details
Step 51: Open the default browser and set it up for malware analysis. This procedure uses Internet Explorer as an example.	1 Make sure the pop-up blocker is turned on. In Internet Explorer, select **Tools** | **Pop-up Blocker** | **Turn on Pop-up Blocker.**  File Edit View Favorites Tools Help Delete browsing history... Ctrl+Shift+Del InPrivate Browsing Ctrl+Shift+P Tracking Protection... ActiveX Filtering Fix connection problems... Reopen last browsing session Add site to Start Screen View downloads Ctrl+J Pop-up Blocker SmartScreen Filter Turn off Pop-up Blocker Pop-up Blocker settings ent lifestyle shopp 2 Select **Tools** | **Internet Options** and for **Home page** enter `about:blank`.  Internet Options General Home page To create home page tabs, type each address on its own line. about:blank ? Security Privacy Content Connections Programs Advance Use current Use default Use new tab Startup 3 Go to the **Advanced** tab of the Internet Options and locate **Security.** 4 Select **Allow active content to run in files on My Computer.**  Settings Multimedia ☑ Enable alternative codecs in HTML5 media elements* ☑ Enable automatic image resizing ☑ Play animations in webpages* ☑ Play sounds in webpages ☐ Show image download placeholders ☑ Show pictures Security ☐ Allow active content from CDs to run on My Computer ☑ Allow active content to run in files on My Computer* ☐ Allow software to run or install even if the signature is General Security Privacy Content Connections Programs 5 Click **OK.**
Step 52: To dynamically analyze Flash files (SWF), install the required version of Adobe Flash.	1 Goto https://community.mcafee.com/docs/DOC-6859. 2 Refer **Adobe flash player installation guidance.docx**.

Step	Details
Step 53: Shut down the VM.	
Step 54: Go to the location that you provided in step 8 to find the VMDK file named as `virtualMachineImage-flat.vmdk`	

Import a VMDK file into Advanced Threat Defense

Before you begin

- You have the VMDK file at hand.
- The operating system has all the applications that you require, such as Microsoft Office applications, Adobe PDF Reader, and so on.
- The VMDK file does not contain any spaces in its file name. If it contains any spaces, the VMDK to image file conversion will fail subsequently.

To create an analyzer VM, you must first import the corresponding VMDK file into Advanced Threat Defense. By default, you can use only SFTP to import the VMDK file. To use FTP, you must enable it using the `set ftp` CLI command. See set ftp on page 363.

> Generally, FTP transfer is faster than SFTP but less secure than SFTP. If your Advanced Threat Defense Appliance is placed in an unsecured network, such as an external network, McAfee recommends you to use SFTP.

Task

1 Open an FTP client.

For example, you can use WinSCP or FileZilla.

2 Connect to the FTP server on Advanced Threat Defense using the following credentials.

- Host: IP address of Advanced Threat Defense.
- Username: atdadmin
- Password: atdadmin
- Port: The corresponding port number based on the protocol you want to use.

3 Upload the VMDK file from the local machine to Advanced Threat Defense.

Convert the VMDK file to an image file

Before you begin

- You have uploaded the VMDK file to Advanced Threat Defense.
- You have admin-user permissions in Advanced Threat Defense.

Task

1. In the Advanced Threat Defense web application, select **Manage** | **Image & Software** | **Image**.
2. In the **Image Management** page, select the VMDK file that you imported from the **VMDK Image** drop-down.
3. Provide a name to the image file.

   > The name that you provide must be between 1 and 20 characters in length and must not contain any spaces. If the image name contains a space, then the conversion to image file fails.

   For malware analysis, you might require multiple analyzer VMs that run on the same operating system but with different applications. For example, you might require a Windows 7 SP1 analyzer VM with Internet Explorer 10 and another Windows 7 SP1 analyzer VM with Internet Explorer 11. If you plan to create multiple analyzer VMs of the same operating system, it is mandatory that you provide an **Image Name**. If you plan to create only one analyzer VM for a specific operating system, then providing the **Image Name** is optional. If you do not provide a name, a default name is assigned to the image file, which you use to view the logs, create VM profile, and so on.

   The default names for the image files are as follows:

   - **winXPsp2**: corresponds to Microsoft Windows XP 32-bit Service Pack 2
   - **winXPsp3**: corresponds to Microsoft Windows XP 32-bit Service Pack 3
   - **win7sp1**: corresponds to Microsoft Windows 7 32-bit Service Pack 1
   - **win7x64sp1**: corresponds to Microsoft Windows 7 64-bit Service Pack 1
   - **win2k3sp1**: corresponds to Microsoft Windows Server 2003 32-bit Service Pack 1
   - **win2k3sp2**: corresponds to Microsoft Windows Server 2003 32-bit Service Pack 2
   - **win2k8sp1**: corresponds to Microsoft Windows Server 2008 R2 Service Pack 1
   - **win8p0x32**: corresponds to Microsoft Windows 8 32-bit
   - **win8p0x64**: corresponds to Microsoft Windows 8 64-bit

   The name that you provide is appended to the default name. Suppose you provide *with_PDF* as the **Image Name** and the operating system is Windows Server 2003 32-bit Service Pack 1. Then the image file is named as *win2k3sp1_with_PDF*.

   > If you attempt to create multiple analyzer VMs of the same operating system, then every time the image file is named using the default name for the operating system. Therefore, the same image file is overwritten every time instead of creating a new analyzer VM of the same operating system. This is why it is mandatory to provide **Image Name** when creating multiple analyzer VMs of the same operating system.

4. Select the corresponding operating system from the **Operating System** drop-down.

5 Click **Convert**.

The time taken for this conversion depends on the size of the VMDK file. For a 15 GB file, an ATD-3000 might take around five minutes.

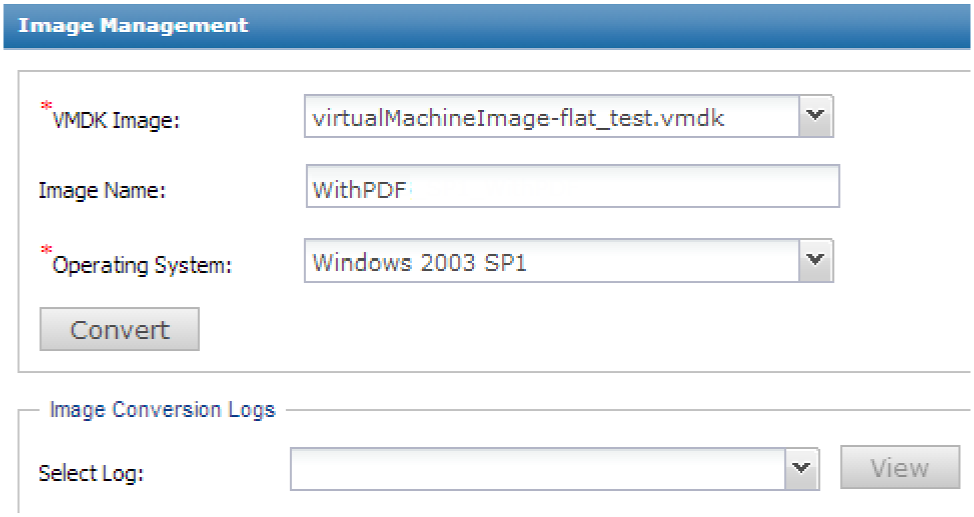


Image Management

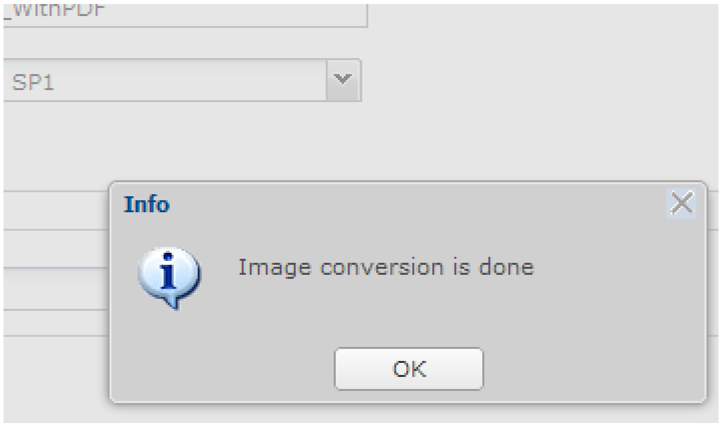
*VMDK Image: virtualMachineImage-flat_test.vmdk

Image Name: WithPDF

*Operating System: Windows 2003 SP1

Figure 5-2 VMDK to image file conversion

After the conversion is complete, a message is displayed.



_WithPDF

SP1

Info

Image conversion is done

Figure 5-3 Confirmation message

6 To view the logs related to image conversion, select the image name from the **Select Log** list and click **View**.

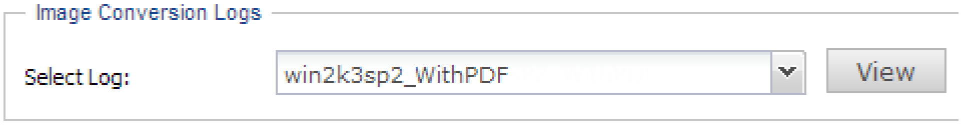


Image Conversion Logs

Select Log: win2k3sp2_WithPDF

Figure 5-4 Select the image file to view the logs

If you had not provided the **Image Name**, then the image file is assigned the default name based on the operating system. If you had provided an **Image Name**, the name that you provided is appended to the default name.

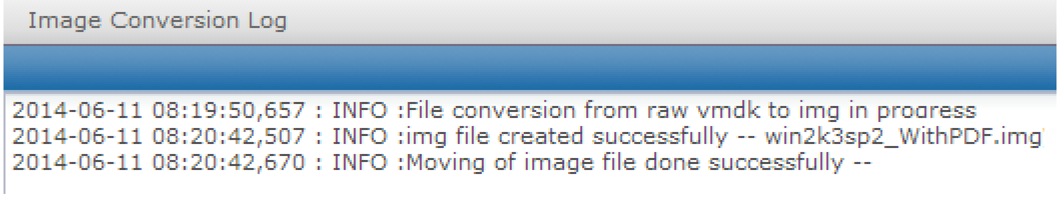


Image Conversion Log

```
2014-06-11 08:19:50,657 : INFO :File conversion from raw vmdk to img in progress
2014-06-11 08:20:42,507 : INFO :img file created successfully -- win2k3sp2_WithPDF.img
2014-06-11 08:20:42,670 : INFO :Moving of image file done successfully --
```

Figure 5-5 Image conversion log entries

Managing VM profiles

After you convert the imported VMDK file to an image file, you create a VM profile for that image file.

You cannot associate this VM profile with any other image file. Similarly, once associated, you cannot change the VM profile for an image file.

VM profiles contain the operating system and applications in an image file. This enables you to identify the images that you uploaded to Advanced Threat Defense and then use the appropriate image for dynamically analyzing a file. You can also specify the number of licenses that you possess for the operating system and the applications. Advanced Threat Defense factors this in when creating concurrent analyzer VMs from the corresponding image file.

You use the Advanced Threat Defense web application to manage VM profiles.

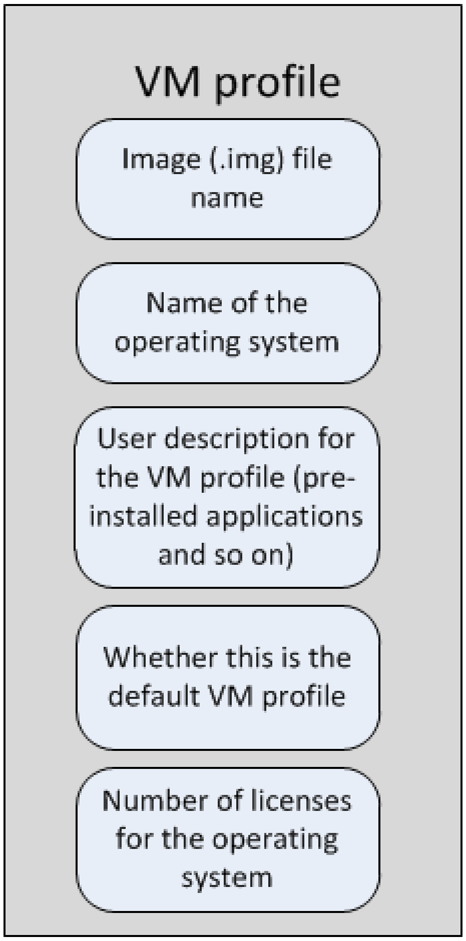

VM profile
Image (.img) file name
Name of the operating system
User description for the VM profile (pre-installed applications and so on)
Whether this is the default VM profile
Number of licenses for the operating system

Figure 5-6 Configurations in a VM profile

View VM profiles

You can view the existing VM profiles in the Advanced Threat Defense web application.

Task

1 Select **Policy** | **VM Profile**.

The currently available VM profiles are listed.

Column name	Definition
Select	Select to edit or delete the corresponding VM profile.
Name	Name that you have assigned to the VM profile.
Licenses	The number of end-user licenses that you possess for the corresponding operating system and applications. This is one of the factors that determine the number of concurrent analyzer VMs on Advanced Threat Defense.
Default	Whether this is a default VM profile.
Size	The size of the image file in megabytes.
Hash	The MD5 hash value of the image file.

2 Hide the unneeded columns.

   a Move the mouse over the right corner of a column heading and click the drop-down arrow.

   b Select **Columns**.

   c Select only the required column names from the list.

   You can click a column heading and drag it to the required position.

3 To sort the records based on a particular column name, click the column heading.

   You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4 To view the complete details of a specific VM Profile, select the record and click **View**.

Create VM profiles

After you have converted the VMDK file to the image format, you can initiate the VM creation and also create the corresponding VM profile.

Each image file that you converted must be associated with only one VM profile. That is, you need one unused image file for each VM profile that you want to create. However, you can convert the same VMDK file image files multiple times. This enables you to create multiple image files from one VMDK file.

Task

1 Select **Policy** | **VM Profile** | **New**

   The **VM Profile** page is displayed.

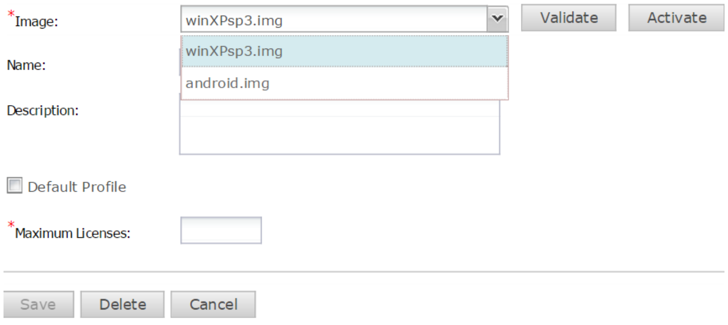


Figure 5-7 Select the image file

2 From the **Image** drop-down, select the one for which you want to create the VM profile.

3 Click **Activate** to create the VM from the selected image file.

   - When you click **Activate**, the Activation window is opened in a new tab or window based on the browser settings.

   This is not related to Windows activation with Microsoft. You must complete Windows activation before you import the VMDK file into Advanced Threat Defense using FTP or SFTP.

A progress bar indicating the VM creation is displayed. Once this is done, the VM boots up.

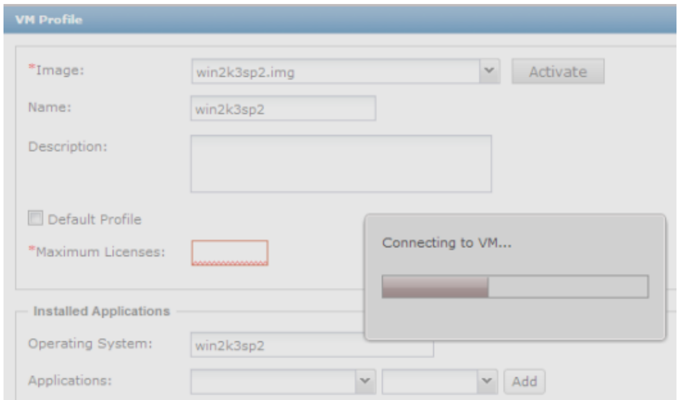


*Image: win2k3sp2.img

Name: win2k3sp2

Description:

☐ Default Profile

*Maximum Licenses:

Operating System: win2k3sp2

Applications:

Connecting to VM...

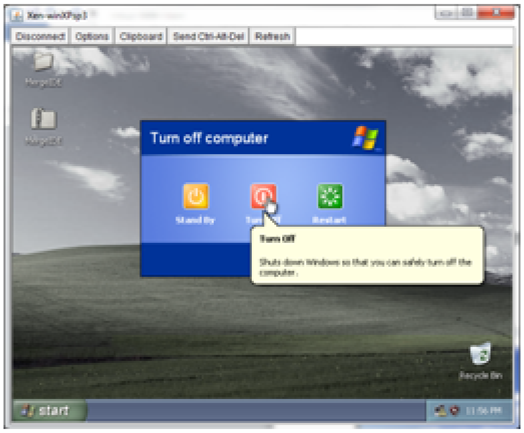
Figure 5-8 Progress of the VM creation

4 Select **Start** | **Control Panel** | **Windows Activation** | **Activate Windows now**. Now, open Microsoft Word and click **Activate**, once **Microsoft Office Activation Wizard** pops up.

> After the aforementioned step, if you want to use a different Ethernet port for malware network access, select **Start** | **Control Panel** | **Network and Internet** | **Network and Sharing Center** and right click on **Properties of TCP/IPv4**. Now, set **Preferred DNS Server**.

> Online Windows Activation needs internet access. An activation packet is sent through the gateway IP that is assigned to the management port. If you have a proxy environment to access external internet, then you need to configure proxy settings on your VM manually, because Advanced Threat Defense proxy settings will not work for Windows Activation packet on your VM. After the activation, the proxy settings on the VM needs to be manually removed.

5 After the VM is up, properly shut it down and close the window or tab.



Turn Off

Shuts down Windows so that you can safely turn off the computer.

Figure 5-9 Shut down the VM

6 Click **Disconnect** once activation is complete.

7 Click **Validate**.

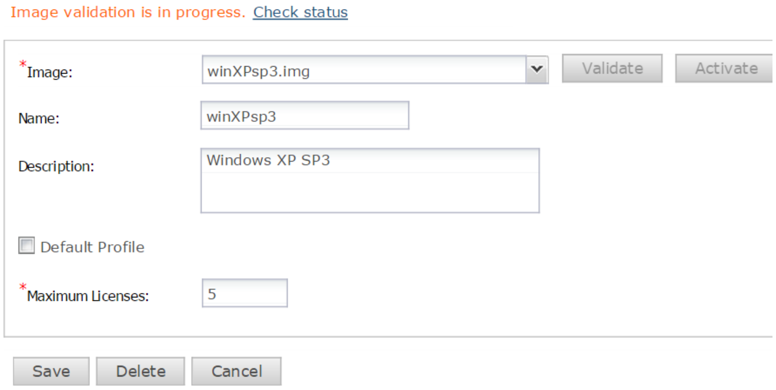


Image validation is in progress. Check status

*Image: winXPsp3.img

Name: winXPsp3

Description: Windows XP SP3

□ Default Profile

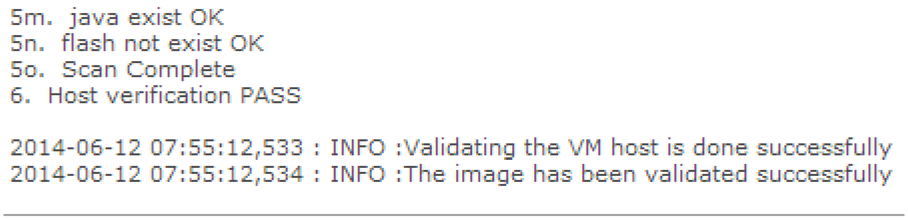
*Maximum Licenses: 5

Figure 5-10 Validating the image file

The following message is displayed, **5n. flash not exist OK**. After importing the VMDK file to Advanced Threat Defense Appliance, the windows VM needs to be reactivated as the MAC ID changes once the software is imported to a different hardware. Refer **KB83738** to resolve the issue.

Once validated, Advanced Threat Defense ensures that the VM is adapted to the Advanced Threat Defense Appliance hardware. Also, it checks if the VM is working fine, configures the required networking details, checks the applications installed, and so on. If the VM is found to work fine, the validation is successful.

Click **Check Status** to view the image validation log. You can proceed to create the VM profile only if the validation is successful. If the validation fails, review the validation log for the reason. Then create a new VMDK with the correct settings and redo the process of creating the analyzer VM.



```
5m.  java exist OK
5n.  flash not exist OK
5o.  Scan Complete
6.  Host verification PASS

2014-06-12 07:55:12,533 : INFO :Validating the VM host is done successfully
2014-06-12 07:55:12,534 : INFO :The image has been validated successfully
```

Figure 5-11 Image validation log

Customer can delete the .img files directly from Advanced Threat Defense interface. This will delete any unnecessary image files stored in the back-end. Only admin role users can delete the image files. Non-admin users cannot delete the file. An image can be deleted only if it is not in use / No vms were created.

Use the following steps to delete unwanted images:

Policy | **VMProfile** | **New** | **Select the .img file from drop-down** | **Delete**

If the selected image is in use, then the following message appears: "The image file is in use and cannot be removed".

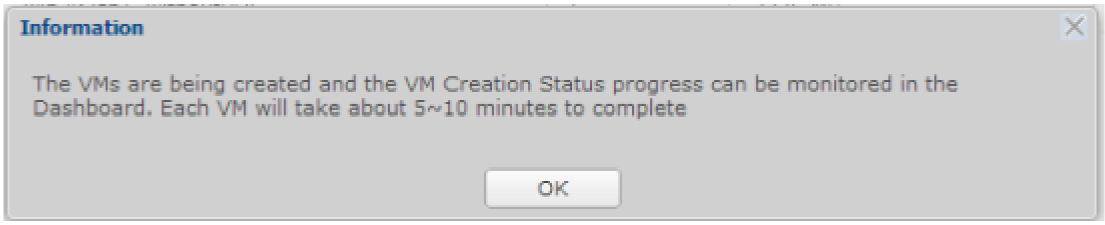
8 Create the VM profile for the VM that you created by entering the appropriate information in the respective fields.

Table 5-4 Option definitions

Option name	Definition
Name	The name of the image file is automatically displayed as the name for the VM profile. You cannot modify it.
Description	Optionally, provide a detailed description of the VM profile.
Default Profile	The first time, you must select it to make the VM profile the default one; subsequently you can select or ignore it. For a file, if the target host environment is not available or if the required analyzer VM is not available, Advanced Threat Defense uses this VM to dynamically analyze the file.
Maximum Licenses	Enter the number of concurrent user licenses that you possess. You must factor in the operating system as well as the applications in the image file. Consider that the image file is a Windows 7 machine with Microsoft Office installed. You have 3 concurrent licenses for Windows 7 and 2 for Microsoft Office. In this case, you must enter 2 as the maximum licenses. This is one of the factors that determine the number of concurrent analyzer VMs that Advanced Threat Defense creates from the image file. The maximum analyzer VMs supported on an ATD-3000 is 30 and on an ATD-6000, it is 60. That is, the cumulative value of **Maximum Licenses** in all the VM profiles must not exceed 30 for an ATD-3000 and 60 for an ATD-6000, including the default Android analyzer VM. So, you can have up to 29 licenses for Windows analyzer VMs in an ATD-3000 and 59 in case of ATD-6000.
Save	Creates the VM profile record with the information you provided. When you click **Save**, the VM creation starts in the background, running as a daemon, and the VM profile is listed in the VM Profile page. Even if the newly created VM profile is listed in the **VM Profile** page, it might take 10-15 minutes before the analyzer VM and VM profile are ready for use.
Cancel	Closes the **VM Profile** page without saving the changes.

9 Monitor the progress of VM creation.

A message is displayed about the VM creation.

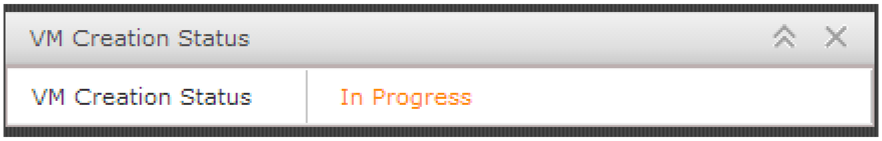


Information

The VMs are being created and the VM Creation Status progress can be monitored in the Dashboard. Each VM will take about 5~10 minutes to complete

You can monitor the progress using the following methods:

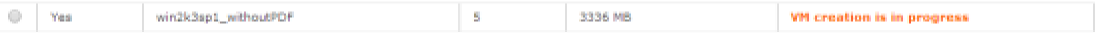
- Select **Dashboard** and check the **VM Creation Status** monitor.



VM Creation Status

VM Creation Status	In Progress

- Select **Policy** | **VM Profile** to view the status against the corresponding VM profile.

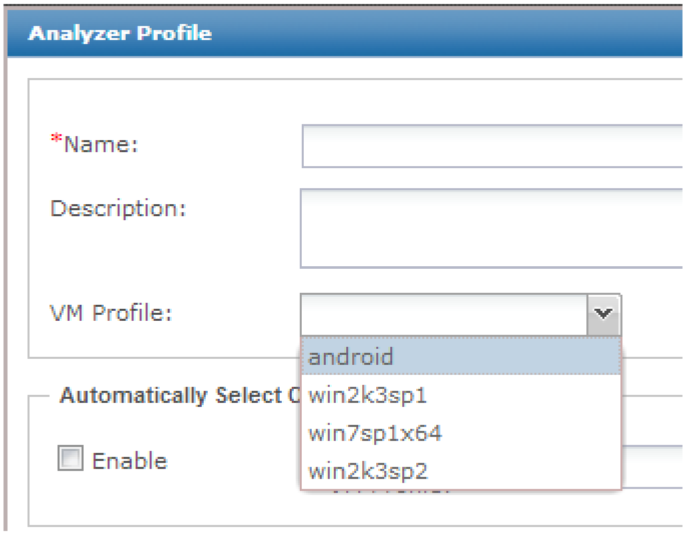


○	Yes	win2k3sp1_withoutPDF	5	3336 MB	VM creation is in progress

If the VM creation fails, the **License** column displays 0. In that case, you need to manually delete the VM profile. Select the VM profile and click **Delete**.

To view the system logs related to VM creation, select **Manage** | **System Log**. an

10 To confirm successful VM profile creation, select **Policy** | **Analyzer Profile** and check if the VM profile that you created is listed in the **VM Profile** drop-down.



Edit VM profiles

Before you begin

To edit a VM profile, either you must have created it or you must have admin-user role.

Task

1 Select **Policy** | **VM Profile**.

The currently available VM profiles are listed.

2 Select the required record and click **Edit**.

The **VM Profile** page is displayed.

3 Make the changes to the required fields and click **Save**.

Delete VM profiles

Before you begin

- To delete a VM profile, either you must have created it or you must have admin-user role.
- Make sure the VM profile you want to delete is not specified in the analyzer profiles.

Task

1. Select **Policy | VM Profile**.

   The currently available VM profiles are displayed.

2. Select the required record and click **Delete**.

3. Click **Yes** to confirm deletion.

View the System log

When you create a VM profile using the **VM Profile** page, Advanced Threat Defense creates an analyzer VM from the image file you selected in the VM profile record. Simultaneously, it prints the related logs, which you can view in the Advanced Threat Defense web application. Through these log entries, you can view what is happening as the analyzer VM is being created. You can use this information for troubleshooting purposes.

- After you click **Save** in the **VM Profile** page, select **Manage | Logs | System** to view the VM creation log entries.

6 Configuring Advanced Threat Defense for malware analysis

After you install Advanced Threat Defense Appliance on your network, you can configure it to analyze malware. For this, you use the Advanced Threat Defense web application. You must have at least the web-access role to configure malware analysis.

This section introduces you to the related terminologies and provides the procedures to set up Advanced Threat Defense for malware analysis.

Contents

Terminologies

Being familiar with the following terminologies facilitates malware analysis using Advanced Threat Defense.

- **Static analysis** — When Advanced Threat Defense receives a supported file for analysis, it first performs static analysis of the file. The objective is to check if it is a known malware in the shortest possible time, and also to preserve the Advanced Threat Defense resources for dynamic analysis. For static analysis, Advanced Threat Defense uses the following resources.

> Static analysis sequence is following.
>
> 1. Local Whitelist > 2. Local Blacklist >3. McAfee GTI / McAfee Gateway Anti-Malware Engine / McAfee Anti-Malware Engine (These three resources are processed in tandem.)

- **Local Whitelist —** This is the list of MD5 hash values of trusted files, which need not be analyzed. This whitelist is based on the McAfee® Application Control database that is used by other solutions in the McAfee suite. This has over 230,000,000 entries.

  The whitelist feature is enabled by default. To disable it, use the `setwhitelist` command. There are commands to manage the entries in the whitelist. The static McAfee® Application Control database cannot be modified. However, you can add or delete entries based on file hash. You can also query the whitelist for a certain file hash to see if it has been added to the database.

  > The default whitelist entries are not periodically updated. However, they might be updated when you upgrade the Advanced Threat Defense software.

  The McAfee products that submit files to Advanced Threat Defense do have the capability to perform custom whitelisting as well. This includes the McAfee Web Gateway and the McAfee Network Security Platform

- **Local Blacklist —** This is the list of MD5 hash values of known malware stored in the Advanced Threat Defense database. When Advanced Threat Defense detects a malware through its heuristic McAfee Gateway Anti-Malware engine or through dynamic analysis, it updates the local blacklist with the file's MD5 hash value. A file is added to this list automatically only when its malware severity as determined by Advanced Threat Defense is medium, high, or very high. There are commands to manage the entries in the blacklist.

- **McAfee GTI —** This is a global threat correlation engine and intelligence base of global messaging and communication behavior, which enables the protection of the customers against both known and emerging electronic threats across all threat areas. The communication behavior includes the reputation, volume, and network traffic patterns. Advanced Threat Defense uses both the IP Reputation and File Reputation features of GTI.

  > DNS must be configured for GTI to run.

  > For File Reputation queries to succeed, make sure Advanced Threat Defense is able to communicate with `tunnel.message.trustedsource.org` over HTTPS (TCP/443). Advanced Threat Defense retrieves the URL updates from `List.smartfilter.com` over HTTP (TCP/80).

  - **Gateway Anti-Malware —** McAfee Gateway Anti-Malware Engine analyzes the behavior of web sites, web site code, and downloaded Web 2.0 content in real time to preemptively detect and block malicious web attacks. It protects businesses from modern blended attacks, including viruses, worms, adware, spyware, riskware, and other crimeware threats, without relying on virus signatures.

    McAfee Gateway Anti-Malware Engine is embedded within Advanced Threat Defense to provide real-time malware detection.

  - **Anti-Malware** — McAfee Anti-Malware Engine is embedded within Advanced Threat Defense. The DAT is updated automatically based on the network connectivity of Advanced Threat Defense.

    Static analysis also involves analysis through reverse engineering of the malicious code. This includes analyzing all the instructions and properties to identify the intended behaviors, which might not surface immediately. This also provides detailed malware classification information, widens the security cover, and can identify associated malware that leverages code re-use.

  > By default, Advanced Threat Defense downloads the updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. Manual update of DAT is not allowed.

- **Dynamic analysis —** In this case, Advanced Threat Defense executes the file in a secure VM and monitors its behavior to check how malicious the file is. At the end of the analysis, it provides a detailed report as required by the user. Advanced Threat Defense does dynamic analysis after the static analysis is done. By default, if static analysis identifies the malware, Advanced Threat Defense does not perform dynamic analysis. However, you can configure Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis. You can also configure only dynamic analysis without static analysis. Dynamic analysis includes the disassembly listing feature of Advanced Threat Defense as well. This feature can generate the disassembly code of PE files for you to analyze the sample further.

- **Analyzer VM —** This is the virtual machine on the Advanced Threat Defense that is used for dynamic analysis. To create the analyzer VMs, you need to create the VMDK file with the required operating system and applications. Then, using SFTP, you import this file into the Advanced Threat Defense Appliance.

  Only the following operating systems are supported to create the analyzer VMs:

  - Microsoft Windows XP 32-bit Service Pack 2
  - Microsoft Windows XP 32-bit Service Pack 3
  - Microsoft Windows Server 2003 32-bit Service Pack 1
  - Microsoft Windows Server 2003 32-bit Service Pack 2
  - Microsoft Windows Server 2008 R2 Service Pack 1
  - Microsoft Windows 7 32-bit Service Pack 1
  - Microsoft Windows 7 64-bit Service Pack 1
  - Microsoft Windows 8.0 Pro 32-bit
  - Microsoft Windows 8.0 Pro 64-bit
  - Android 2.3 by default. You can upgrade it to Android 4.3. See Upgrade the Android analyzer VM on page 52.

  All of the above Windows operating systems can be in English, Chinese Simplified, Japanese, German, or Italian.

  > The only pre-installed analyzer VM is the Android VM.

You must create analyzer VMs for Windows. You can create different VMs based on your requirements. The number of analyzer VMs that you can create is limited only by the disk space of the Advanced Threat Defense Appliance. However, there is a limit as to how many of them can be used concurrently for analysis. The number of concurrent licenses that you specify also affects the number of concurrent instances for an analyzer VM.

- **VM profile —** After you upload the VM image (.vmdk file) to Advanced Threat Defense, you associate each of them with a separate VM profile. A VM profile indicates what is installed in a VM image and the number of concurrent licenses associated with that VM image. Using the VM image and the information in the VM profile, Advanced Threat Defense creates the corresponding number of analyzer VMs. For example, if you specify that you have 10 licenses for Windows XP SP2 32-bit, then Advanced Threat Defense understands that it can create up to 10 concurrent VMs using the corresponding .vmdk file.
- **Analyzer profile —** This defines how to analyze a file and what to report. In an analyzer profile, you configure the following:
  - VM profile
  - Analysis options
  - Reports you wish to see after the analysis
  - Password for zipped sample files
  - Minimum and maximum execution time for dynamic analysis

  You can create multiple analyzer profiles based on your requirements. For each Advanced Threat Defense user, you must specify a default analyzer profile. This is the analyzer profile that is used for all files uploaded by the user. Users who use the Advanced Threat Defense web application to manually upload files for analysis, can choose a different analyzer profile at the time of file upload. Always, the analyzer profile selected for a file takes precedence over the default analyzer profile of the corresponding user.

  To dynamically analyze a file, the corresponding user must have the VM profile specified in the user's analyzer profile. This is how the user indicates the environment in which Advanced Threat Defense should execute the file. You can also specify a default Windows 32-bit and a 64-bit VM profile.
- **User —** A Advanced Threat Defense user is one who has the required permissions to submit files to Advanced Threat Defense for analysis and view the results. In case of manual submission, a user could use the Advanced Threat Defense web application or an FTP client. In case of automatic submission, you integrate McAfee products such as McAfee Network Security Platform or McAfee Web Gateway with Advanced Threat Defense. Then when these products detect a file download, they automatically submit the file to Advanced Threat Defense before allowing the download to complete. So, for these products default user profiles are available in Advanced Threat Defense.

  For each user, you define the default analyzer profile, which in turn can contain the VM profile. If you use the Advanced Threat Defense for uploading files for analysis, you can override this default profile at the time of file submission. For other users, Advanced Threat Defense uses the default profiles.

High-level steps for configuring malware analysis

This section provides the high-level steps on how to configure Advanced Threat Defense for malware analysis and reporting:

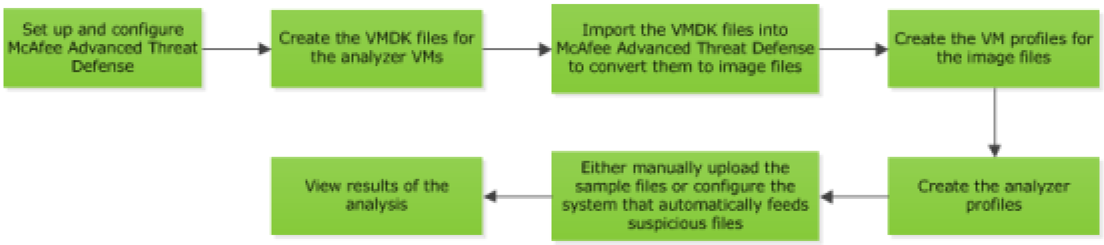

Set up and configure McAfee Advanced Threat Defense
Create the VMDK files for the analyzer VMs
Import the VMDK files into McAfee Advanced Threat Defense to convert them to image files
Create the VM profiles for the image files
Create the analyzer profiles
Either manually upload the sample files or configure the system that automatically feeds suspicious files
View results of the analysis

Figure 6-1 Summarized steps for configuring malware analysis

1. Set up the Advanced Threat Defense Appliance and ensure that it is up and running.
   - Based on your deployment option, make sure the Advanced Threat Defense Appliance has the required network connections. For example, if you integrate it with Network Security Platform, make sure the Sensor, Manager, and the Advanced Threat Defense Appliance are able to communicate with each other.
   - Make sure the required static analysis modules, such as the McAfee Gateway Anti-Malware Engine are up-to-date.
2. Create the analyzer VMs and the VM profiles. See Creating analyzer VM on page 4.
3. Create the analyzer profiles that you need. See Managing analyzer profiles on page 239.
4. If you want Advanced Threat Defense to upload the results to an FTP server, configure it and have the details with you before you create the profiles for the corresponding users.
5. Create the required user profiles. See Add users on page 39.
6. Log on to Advanced Threat Defense web application using the credentials of a user you created and upload a sample file for analysis. This is to check if you have configured Advanced Threat Defense as required. See Upload files for analysis using Advanced Threat Defense web application on page 284.
7. In the **Analysis Status** page, monitor the status of the analysis. See Configure the Analysis Status page on page 293
8. After the analysis is complete, view the report in the **Analysis Results** page. See View the analysis results on page 295.

How Advanced Threat Defense analyzes malware?

This section explains a typical workflow when Advanced Threat Defense analyzes files for malware.

Consider that you have uploaded a file manually using Advanced Threat Defense web application:

1. Assuming the file format is supported, Advanced Threat Defense unpacks the file and calculates the MD5 hash value.
2. Advanced Threat Defense applies the analyzer profile that you specified during file upload.
3. Based on the configuration in the analyzer profile, it determines the modules to use for static analysis and checks the file against those modules.

4 If the file is found to be malicious during static analysis, Advanced Threat Defense stops further analysis and generates the required reports. This, however, depends on how you have configured the corresponding analyzer profile.

5 If the static analysis does not report any malware or if you had configured Advanced Threat Defense to perform dynamic analysis regardless of the results from static analysis, Advanced Threat Defense initiates dynamic analysis for the file.

6 It executes the file in the corresponding analyzer VMs and records every behavior. The analyzer VM is determined based on the VM profile in the analyzer profile.

7 If the file is fully executed or if the maximum execution period expires, Advanced Threat Defense prepares the required reports.

8 After dynamic analysis is complete, it sets the analyzer VMs to their baseline version so that they can be used for the next file in queue.

Internet access to sample files

When being dynamically analyzed, a sample might access a resource on the Internet. For example, the sample might attempt to download additional malicious code or attempt to upload information that it collected from the host machine (in this case, the analyzer VM). You can configure Advanced Threat Defense to provide network services to analyzer VMs so that the network activities of a sample file can be analyzed.

Providing Internet access to samples enables Advanced Threat Defense to analyze the network behavior of a sample and also determine the impact of the additional files downloaded from the Internet. Some malware might try to determine if they are being executed in a sandbox by requesting for Internet access and then alter their behavior accordingly.

When an analyzer VM is created, Advanced Threat Defense makes sure that the analyzer VM has the configurations to communicate over a network when required.

You can control granting real network access to an analyzer VM through a setting in the analyzer profiles. Network services are provided regardless of the method used to submit the sample. For example, it is provided to samples submitted manually using the Advanced Threat Defense web application as well as samples submitted by the integrated products.

The following is the high-level process flow when a sample accesses a resource on the Internet.

1 A sample attempts to access a resource on the Internet.

2 Advanced Threat Defense checks if the Internet connectivity is enabled in the corresponding analyzer profile used for this analysis.

3 Based on whether Internet connectivity is enabled or not, Advanced Threat Defense determines the mode in which network services are to be provided.

- Simulator mode — If Internet connectivity is not enabled in the analyzer profile, this mode is used. Advanced Threat Defense can represent itself as being the target resource. For example, if the sample attempts to download a file through FTP, Advanced Threat Defense simulates this connection for the analyzer VM.

- Real Internet mode — This mode requires the management port (eth-0), eth-1, eth-2 or eth-3 to have access to the Internet. If Internet connectivity is enabled in the analyzer profile, Advanced Threat Defense uses this mode. Advanced Threat Defense provides real Internet connection through the management port by default, which is publicly routed or directed towards your enterprise firewall as per your network configuration. Because the traffic from an analyzer VM could be malicious, you might want to segregate this traffic away from your production network. In this case, you can use Advanced Threat Defense's eth-1, eth-2, or eth-3 provide Internet access to the analyzer VM.

4 Regardless of the mode used, Advanced Threat Defense logs all the network activities. However, the types of reports generated might vary based on the mode.

- Network activities are summarized and presented in the Analysis Summary report. You can find the DNS queries and socket activities under network operations. You can find all the network activities in the **Network Simulator** section of the report.

- The dns.log report also contains the DNS queries made by the sample.

- The packet capture of the network activities is provided in the NetLog folder within the Complete Results zip file.

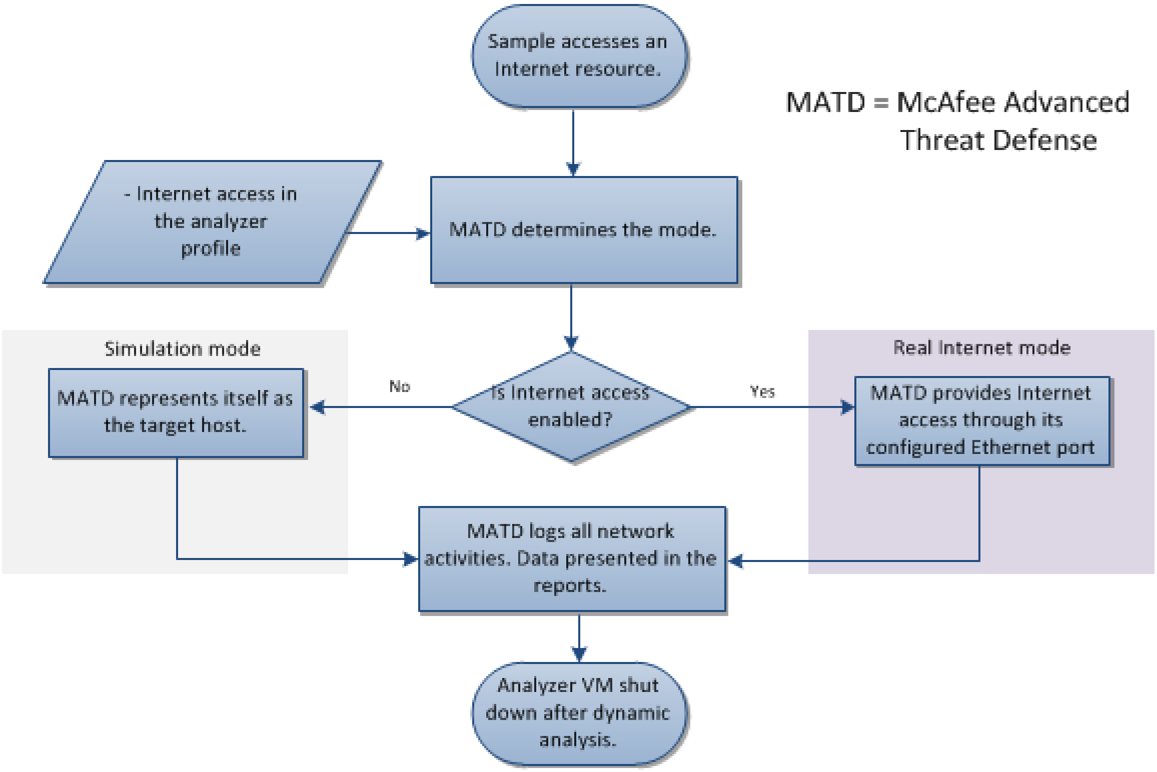
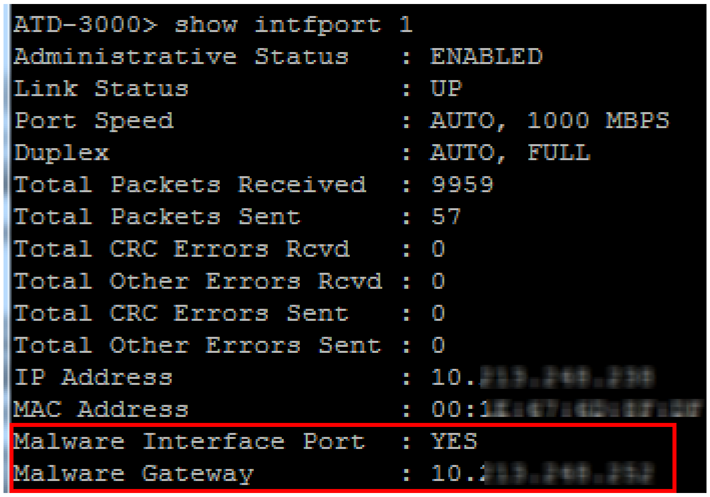

Sample accesses an Internet resource.
MATD = McAfee Advanced Threat Defense
- Internet access in the analyzer profile
MATD determines the mode.
Simulation mode
Real Internet mode
MATD represents itself as the target host.
No
Is Internet access enabled?
Yes
MATD provides Internet access through its configured Ethernet port
MATD logs all network activities. Data presented in the reports.
Analyzer VM shut down after dynamic analysis.

Figure 6-2 Internet access to samples - process flow

Recall that Advanced Threat Defense uses its management port (eth-0) by default to provide Internet access to samples. You can also configure a different port for this purpose.

To enable a different Ethernet port for malware network access, follow the procedure below:

1. Log on to the Advanced Threat Defense CLI and enable the required port. For example, `set intfport 1 enable` to enable eth-1 port.
2. Set the required IP address and subnet mask for the port. For example, `set intfport 1 10.10.10.10 255.255.255.0`
3. For the Ethernet port, set the gateway through which you want to route the Internet access. For example, `set malware-intfport 1 gateway 10.10.10.252`
4. Run the `show intfport <port number>` command for the port to check if it is configured for malware Internet access. For example, `show intfport 1`. Verify the `Malware Interface Port` and `Malware Gateway` entries.



```
ATD-3000> show intfport 1
Administrative Status    : ENABLED
Link Status              : UP
Port Speed               : AUTO, 1000 MBPS
Duplex                   : AUTO, FULL
Total Packets Received   : 9959
Total Packets Sent       : 57
Total CRC Errors Rcvd    : 0
Total Other Errors Rcvd  : 0
Total CRC Errors Sent    : 0
Total Other Errors Sent  : 0
IP Address               : 10.[redacted]
MAC Address              : 00:1[redacted]
Malware Interface Port   : YES
Malware Gateway          : 10.[redacted]
```

- To revert to the managment port (eth-0) for malware Internet access, run `set malware-intfport mgmt` in the CLI. Advanced Threat Defense uses its management port IP and the corresponding default gateway to provide Internet access to samples.
- Suppose you configured eth-1 for malware Internet access but now you want to use eth-2. Then, follow the above procedure for eth-2. Eth-2 is set as the port for Internet access for malware.
- Suppose you configured eth-1 for Internet access but now you want to use eth-1 but with a different IP address or gateway. Then, repeat the procedure but with the new IP address or gateway.
- The `route add network` command is for general Advanced Threat Defense traffic. Whereas, `set malware-intfport` is for Internet traffic from an analyzer VM. So, the `route add network` and the `set malware-intfport` commands do not affect each other.

Managing analyzer profiles

When a file is manually or automatically submitted to Advanced Threat Defense for analysis, it uses the corresponding analyzer profile to determine how the file needs to be analyzed and what needs to be reported in the analysis results. You specify the VM profile in the analyzer profile. You also define how the file is to be analyzed for malware and the reports to be published. Thus, an analyzer profile contains all the critical user-configuration on how to analyze a file.

You use the Advanced Threat Defense web application to manage analyzer profiles.

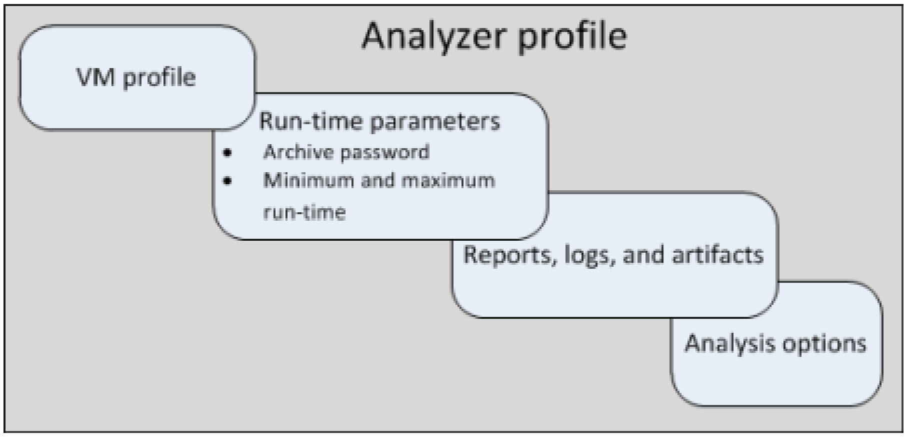


Figure 6-3 Contents of an analyzer profile

View analyzer profiles

Based on your user role, you can view the existing analyzer profiles in the Advanced Threat Defense web application.

Task

1 Select **Policy** | **Analyzer Profile**.

If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

Column name	Definition
Select	Select to edit or delete the corresponding analyzer profile.
Name	Name that you have assigned to the analyzer profile.
Description	The description of the characteristics of the analyzer profile.
OS Name	Corresponds to the name of the VM profile specified in the analyzer profile.
Automatically Select OS	Indicates if you have selected the **Automatically Select OS** option in the analyzer profile.

2 Hide the unneeded columns.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

You can click a column heading and drag it to the required position.

3. To sort the records based on a particular column name, click the column heading.

   You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

4. To view the complete details of a specific analyzer profile, select the record and click **View.**

Create analyzer profiles

Before you begin

- If you intend to select the dynamic analysis option in the analyzer profile, make sure that you have created the required VM profile. VM profiles are also required if you want to use the **Automatically Select OS** option.
- If you want to enable Internet access to samples, then you need admin user privileges.

Task

1 Select **Policy** | **Analyzer Profile** | **New**.

2 Enter the appropriate information in the respective fields.

Option name	Definition
Name	Enter the name for the analyzer profile. It should allow you to easily identify the characteristics of that analyzer profile.
Description	Optionally, provide a detailed description of the analyzer profile.
VM Profile	Select the VM profile Advanced Threat Defense must use for dynamically analyzing a file.
Automatically Select OS	If you want Advanced Threat Defense to automatically select the VM profile for Windows 32-bit and Windows 64-bit, select **Enable** and then select the VM profiles from the **Windows 32-bit VM Profile** and **Windows 64-bit VM Profile**. Consider that for **VM Profile**, you have selected Android. You have enabled **Automatically Select OS**. For **Windows 32-bit VM Profile**, you have selected Windows XP SP3 and for **Windows 64-bit VM Profile**, you have selected Windows 7 SP1 64-bit. Now, when an .apk file is detected, the Android analyzer VM is used for dynamically analyzing the file. Similarly, for a PE32 file, Windows XP SP3 is used. For a PE64 file, Windows 7 SP1 64-bit analyzer VM is used. If Advanced Threat Defense is unable to determine the operating system for this analyzer profile or if the determined analyzer VM is not available, it uses the VM mentioned in the **VM Profile** field. ! Once Windows 64-bit is set as default VM, PE32 files go into Windows 64-bit VM and not into Windows 32-bit VM.
Archive Password	Enter the password for Advanced Threat Defense to unzip a password-protected malware sample.
Confirm Password	Re-enter the password for confirmation.
Minimum Run Time (sec)	Specify the minimum time duration for which Advanced Threat Defense should dynamically analyze the sample. The default value is 5 seconds. The maximum value allowed is 600 seconds. If the file stops executing before this time period, dynamic analysis is stopped.
Maximum Run Time (sec)	Specify the maximum time duration for which Advanced Threat Defense should dynamically analyze the sample. The default value is 180 seconds. The maximum value allowed is 600 seconds. If the file does not stop execution before this time period expires, the dynamic analysis is stopped.
Analysis Summary	Select to include the Analysis Summary report in the analysis results. See View the Threat Analysis report on page 298.
Packet captures	Select to capture the network packets if the file attempts to communicate during dynamic analysis. The pcap file is provided in the complete results zip file.
Dropped Files	Select to generate the Files Created in Sandbox report. See Dropped files report on page 304.
Disassembly Results	Select if you want Advanced Threat Defense to generate the disassembly code of PE files. See Disassembly Results on page 304.
Logic Path Graph	Select to generate Logic Path Graph report. See Logic Path Graph on page 305.
User API Log	This report provides Windows user-level DLL API calls made directly by the malware sample during dynamic analysis. See User API Log on page 310.

Option name	Definition
Local Black List	Select if you want Advanced Threat Defense to check the file's MD5 hash value with the list of black-listed MD5 hash values in its local database.
Anti-Malware	Select if you want Advanced Threat Defense to scan the file using McAfee Anti-Malware Engine.
GTI File Reputation	Select if you want Advanced Threat Defense to check the file's MD5 hash value with McAfee GTI. Make sure Advanced Threat Defense is able to communicate with McAfee GTI, which is on the cloud.
Gateway Anti-Malware	Select if you want Advanced Threat Defense to check the file using McAfee Gateway Anti-Malware Engine.
Sandbox	Select if you want the file to be dynamically analyzed. A file is not dynamically analyzed if any of the static methods report it as a malware or a white-listed file. If you want to dynamically analyze the file regardless of the result from static analysis, select **Run All Selected** as well. Make sure you have selected the VM profile and the **Runtime Parameters**.
Skip files if previously analyzed	Select if you want Advanced Threat Defense to skip analysis of a file if the same has been previously analyzed.
Custom Yara Scanner	Select if you want Advanced Threat Defense to check the file using Custom Yara Scanner rules.
Continue to run all engines even after file is found malicious	Select if you want Advanced Threat Defense to analyze the file using all the selected analyze options regardless of the result from any specific method.
Enable Malware Internet Access	Select to provide Internet access to samples when they attempt to access a resource on the Internet. To enable this option, the **Sandbox** option under Analyzer Options must be enabled. Also, you must have admin role privileges to select or deselect **Enable Malware Internet Access**. Because the sample being analyzed could potentially be a malware, selecting the **Enable Malware Internet Access** option involves the risk of malicious traffic propagating out of your network. A disclaimer message is displayed when you select this option, and you must click **OK** to proceed. Also, administrator can configure proxy setting for malware in case there is a proxy server in their network.
Save	Creates the analyzer profile record with the information you provided.
Cancel	Closes the **Analyzer Profile** page without saving the changes.

Edit analyzer profiles

Task

1. Select **Policy** | **Analyzer Profile**.

   If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

2. Select the required record and click **Edit.**

   The **Analyzer Profile** page is displayed.

3. Make the changes to the required fields and click **Save.**

   The changes affect the corresponding users even if they are currently logged on.

Delete analyzer profiles

Before you begin

Make sure the users to whom you have assigned this analyzer profile are not currently logged on to McAfee Advanced Threat Defense.

Task

1. Select **Policy** | **Analyzer Profile**.

   If you have web access, you can view only the analyzer profiles that you created. If you have admin access, you can view all the analyzer profiles currently in the database.

2. Select the required record and click **Delete.**

3. Click **Yes** to confirm deletion.

Integration with McAfee ePO for OS profiling

Integrating Advanced Threat Defense and McAfee ePO enables Advanced Threat Defense to correctly identify the target host environment and use the corresponding analyzer VM for dynamic analysis.

To determine the analyzer VM for a file submitted by Network Security Platform or McAfee Web Gateway, Advanced Threat Defense uses the following sources of information in the same order of priority:

1. Advanced Threat Defense queries McAfee ePO for the operating system of a host based on its IP address. If information from this source or the corresponding analyzer VM is not available, it goes to the next source.

2. If Device Profiling is enabled, the Sensor provides the operating system and application details when forwarding a file for analysis. If information from this source or the corresponding analyzer VM is not available, it goes to the next source.

3. From the analyzer profile in the corresponding user record, Advanced Threat Defense determines the VM profile. If information from this source or if the corresponding analyzer VM is not available, it goes to the next source.

4. You can select a VM profile in your setup as the default.

When Advanced Threat Defense receives host information for a particular IP address from McAfee ePO, it caches this detail.

- The cached IP address to host information data has a time to live (TTL) value of 48 hours.
- For the first 24 hours, Advanced Threat Defense uses just the host information in the cache.
- For the second 24 hours, Advanced Threat Defense uses the host information from the cache but also queries McAfee ePO and updates its cache. This updated information is valid for the next 48 hours.
- If the cached information is more than 48 hours old, it treats it as if there is no cached information for the corresponding IP address. That is, it attempts to find the information from other sources and also sends a query to McAfee ePO.

The following explains how Advanced Threat Defense collaborates with McAfee ePO.

1. Network Security Platform or McAfee Web Gateway sends a file to Advanced Threat Defense for analysis. When Network Security Platform sends a file, the IP address of the target host is also sent.
2. Advanced Threat Defense checks its cache to see if there is a valid operating system mapped to that IP address.
3. If it is the first time that a file for that IP address is being analyzed, there is no information in the cache. So, it determines the analyzer VM from the device profiling information in case of Network Security Platform and user record in case of McAfee Web Gateway. Simultaneously, it sends a query to McAfee ePO for host information based on the IP address.
4. McAfee ePO forwards the host information to Advanced Threat Defense, which is cached for further use.

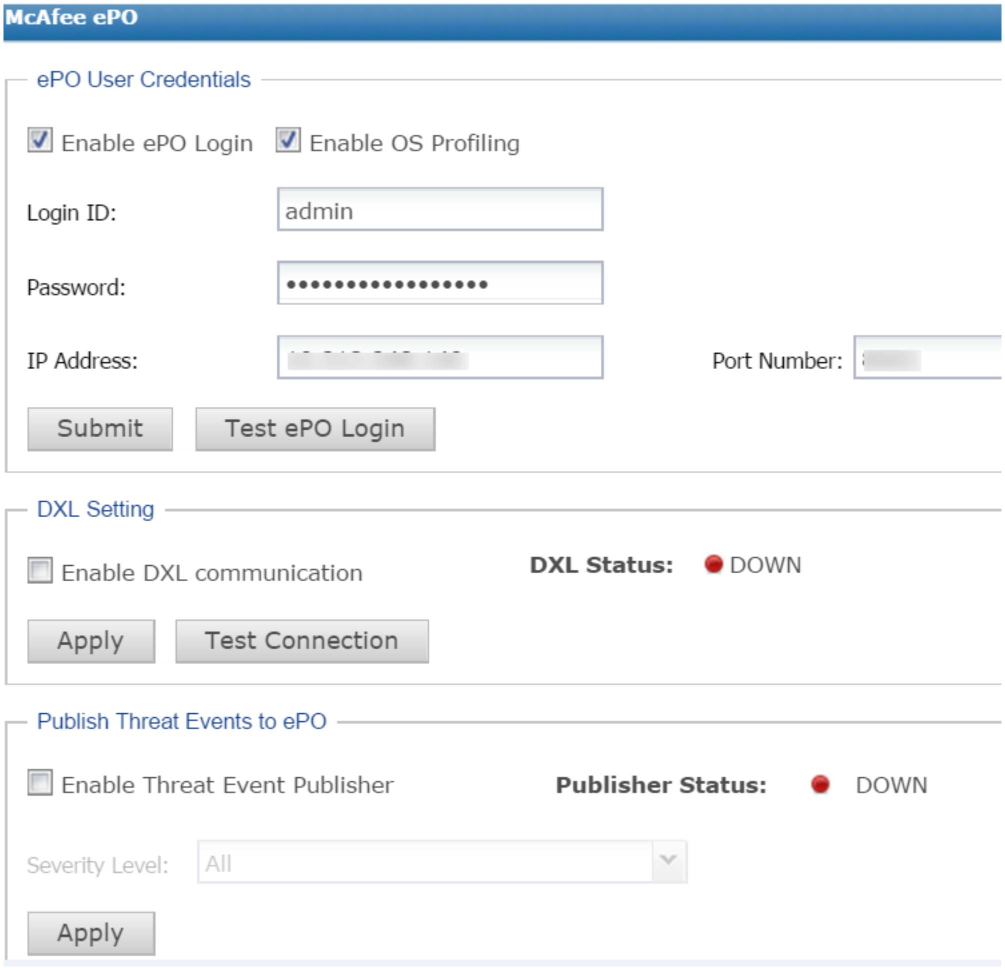
Configure McAfee ePO integration

Integration with McAfee ePO enables McAfee ePO to gather information such as the operating system, browsers installed and so on, on the target host. Advanced Threat Defense uses this information to select the best analyzer VM for dynamic analysis.

Task

1 Select **Manage** | **Configuration** | **ePO Login/DXL Setting**.

The **ePO Login/DXL Setting** page displays.



McAfee ePO

ePO User Credentials

☑ Enable ePO Login ☑ Enable OS Profiling

Login ID: admin

Password: ••••••••••••••••••

IP Address: [redacted] Port Number: [redacted]

DXL Setting

□ Enable DXL communication DXL Status: ● DOWN

Publish Threat Events to ePO

□ Enable Threat Event Publisher Publisher Status: ● DOWN

Severity Level: All

2 Select **Enable ePO Login**.

3 If you require OS profiling service from McAfee ePO, select **Enable OS Profiling**.

4 Enter the details in the appropriate fields.

Option	Definition
Login ID	Enter the McAfee ePO logon name that Advanced Threat Defense uses to access the McAfee ePO server. McAfee recommends that you create a McAfee ePO user account with View-only permissions required for integration.
Password	Enter the password corresponding to the **Logon ID** that you entered.
IP Address	Enter the IPv4 address of the McAfee ePO server. Contact your McAfee ePO administrator for the IP address.
Port Number	Specify the HTTPS listening port on the McAfee ePO server used for the Advanced Threat Defense - McAfee ePO communication. Contact your McAfee ePO administrator for the port number.
Test ePO Login	Click to verify if Advanced Threat Defense is able to reach the configured McAfee ePO server over the specified port.
Submit	Click to save the configuration and enable Advanced Threat Defense - McAfee ePO integration. Make sure that the test connection is successful before you click **Submit**.

Configure McAfee ePO integration to publish threat events

Integrating Advanced Threat Defense and McAfee ePO enables Advanced Threat Defense to send relevant data about submitted samples to McAfee ePO. Users can select the severity level of files for which the data needs to be captured. This storage of information in McAfee ePO facilitates debugging and support activities.

> Users must install the *ATDThreatEvent* extension on McAfee ePO in order to facilitate publishing of threat events by Advanced Threat Defense. Integration with McAfee ePO to publish threat events is supported with McAfee ePO 5.1.1 or later.

The following data is sent to McAfee ePO from Advanced Threat Defense:

- ATD s/w version
- Job ID
- Task ID
- ATD IP address
- Source IP address
- IOC (Indicators of compromise) file
- MD5 value
- Time stamp
- Size
- Severity

Configure McAfee ePO integration to publish threat event

Integrating Advanced Threat Defense and McAfee ePO enables Advanced Threat Defense to send relevant data about submitted samples to McAfee ePO. Users can select the severity level of files for which the data needs to be captured. This storage of information in McAfee ePO facilitates debugging and support activities.

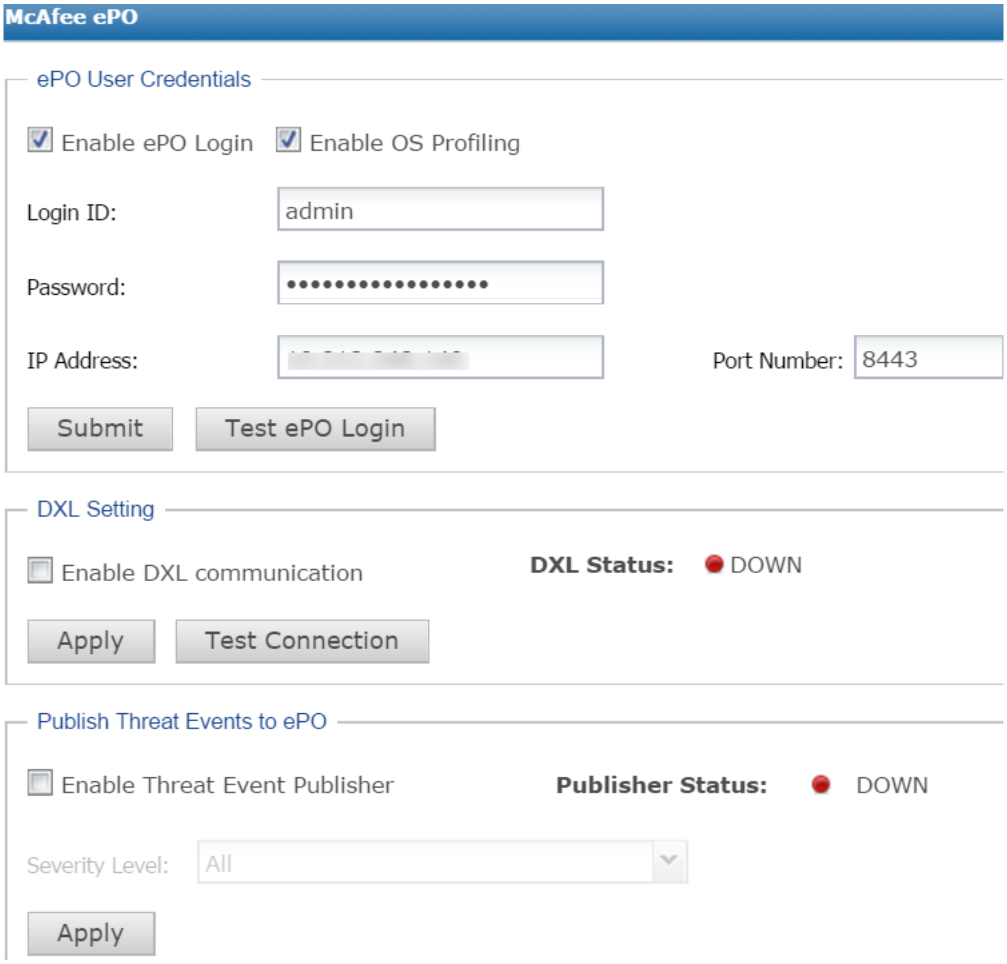
> Users must install the *ATDThreatEvent* extension on McAfee ePO in order to facilitate publishing of threat events by Advanced Threat Defense. Integration with McAfee ePO to publish threat events is supported with McAfee ePO 5.1.1 or later.

The following data is sent to McAfee ePO from Advanced Threat Defense:

- ATD s/w version
- Job ID
- Task ID
- ATD IP address
- Source IP address
- IOC (Indicators of compromise) file
- MD5 value
- Time stamp
- Size
- Severity

Task

1 Select **Manage | ePO login/DXL Setting**.



McAfee ePO

ePO User Credentials

☑ Enable ePO Login ☑ Enable OS Profiling

Login ID: admin

Password: •••••••••••••••••

IP Address: [redacted] Port Number: 8443

DXL Setting

□ Enable DXL communication **DXL Status:** ● DOWN

Publish Threat Events to ePO

□ Enable Threat Event Publisher **Publisher Status:** ● DOWN

Severity Level: All

2 Enter the details in the **ePO User Credentials** and **DXL Setting** areas.

3. In the **Publish Threat Events to ePO** area:
   - Select **Enable Threat Event Publisher**
   - From the **Severity Level** drop-down list, select a severity level based on your requirement
4. Click **Apply**. When the **Publish Threat Events Setting updated successfully** message appears, click **OK**.

> After you click the **Apply** tab, Advanced Threat Defense checks if connection between Advanced Threat Defense and McAfee ePO broker channel is established or not.

> The **Publisher Status** indicator tells whether Advanced Threat Defense is publishing reports to **McAfee ePO** or not.

See also Configure McAfee ePO integration on page 244

Integration with Data Exchange Layer

McAfee Data Exchange Layer (McAfee DXL) includes client software and one or more brokers that allow bidirectional communication between endpoints on a network. The McAfee DXL client is installed on each managed endpoint so that threat information can be shared immediately with all other services and devices, reducing the spread of threats.

Integrating Advanced Threat Defense with McAfee DXL enables Advanced Threat Defense to send the analysis report of the samples analyzed at Advanced Threat Defense to the McAfee DXL broker. Analysis reports of samples that meet the following are sent to McAfee DXL:

- Portable executable (PE) files with a severity score greater than or equal to 2
- Non-PE files with a severity score greater than or equal to 3

These analysis reports are published to a topic located at /mcafee/event/atd/file/report on the McAfee DXL broker. Clients such as Security Information and Event Management (SIEM) that subscribe to this topic can fetch analysis reports from McAfee DXL broker to build a robust security reputation database. Subscribing clients can refer to this database and treat files entering their network according to the analysis report of the files.

1. Advanced Threat Defense gets the sample files from different channels like Network Security Platform, Web Gateway, and so on for analysis.
2. The analysis summary is then sent to the McAfee DXL broker for further on-demand distribution to subscribing clients.

   The following diagram explains Advanced Threat Defense and McAfee DXL integration.

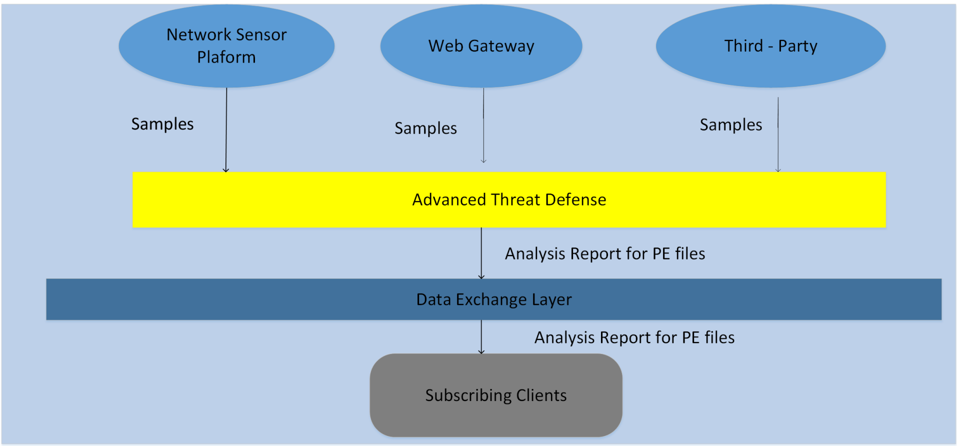


Figure 6-4 Advanced Threat Defense - Data Exchange Layer Integration

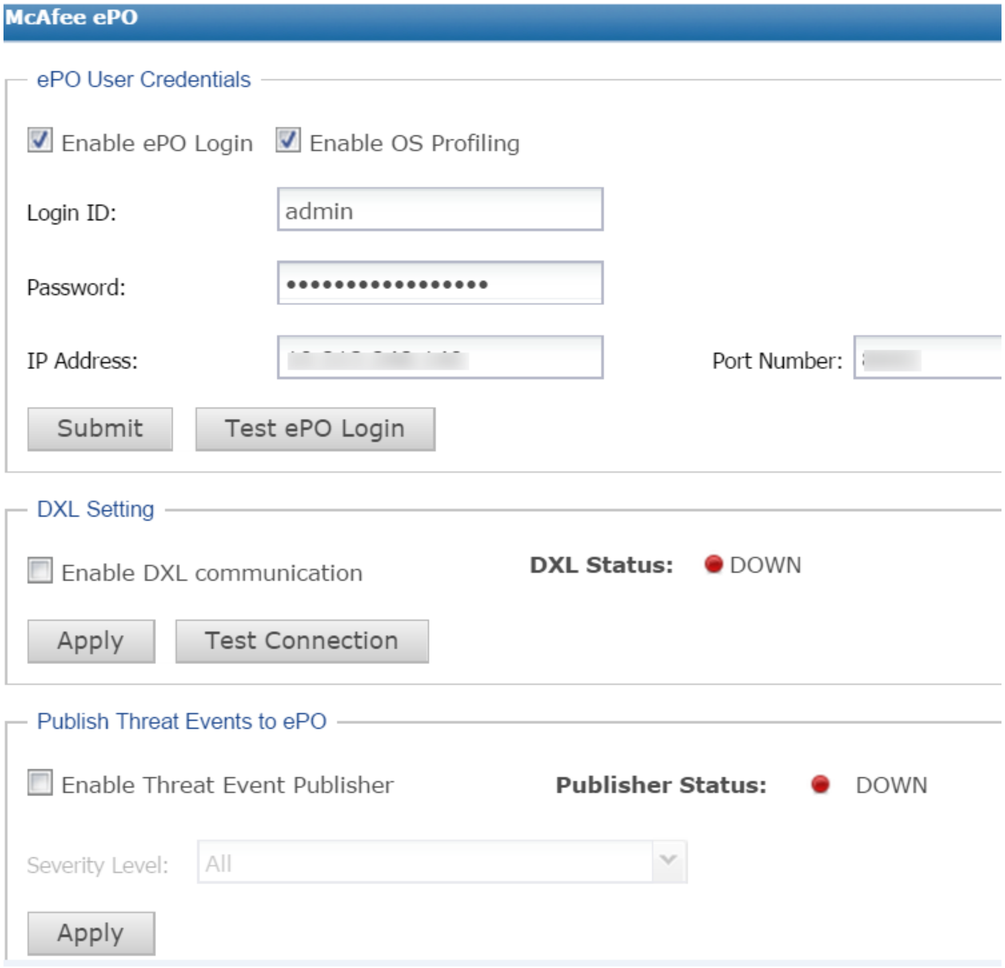
If you want your Advanced Threat Defense to have exclusive rights to publish on the Advanced Threat Defense topic, then you must install the *ATDDXLTagging* extension on McAfee ePO. This restricts publishing on the Advanced Threat Defense topic by any other sender.

McAfee DXL integration with McAfee ePO is supported with McAfee ePO 5.1.1 or later.

Configure Data Exchange Layer integration

Task

1 Select **Manage** | **ePO login/DXL Setting**. The **McAfee ePO** page is displayed.



McAfee ePO

ePO User Credentials

☑ Enable ePO Login ☑ Enable OS Profiling

Login ID: admin

Password: •••••••••••••••••

IP Address: [redacted] Port Number: [redacted]

DXL Setting

□ Enable DXL communication **DXL Status:** ● DOWN

Publish Threat Events to ePO

□ Enable Threat Event Publisher **Publisher Status:** ● DOWN

Severity Level: All

2 Enter the details in the appropriate fields.

3 In **DXL Setting** area, select **Enable DXL communication**.

4 Click **Test Connection**. When a **Test connection is successful** message appears, click **Apply**.

> Once you click on **Test Connection** tab, Advanced Threat Defense checks if connection between Advanced Threat Defense to **DXL** broker channel is established or not.

> **DXL Status** indicator tells whether Advanced Threat Defense is publishing reports to **DXL** broker or not.

Integration with Threat Intelligent Exchange

Integration of Advanced Threat Defense with Threat Intelligent Exchange (TIE) helps Advanced Threat Defense to get the TIE Enterprise Reputation and the McAfee GTI Reputation from the TIE server through the DXL channel for the samples submitted to Advanced Threat Defense. If the DXL channel is enabled and the McAfee GTI Reputation is configured in the Analyzer Profile, Advanced Threat Defense does a file reputation lookup (McAfee GTI/TIE Enterprise Reputation) for the submitted samples through the DXL channel. If the TIE Enterprise Reputation is configured by the administrator on the McAfee ePO, the Threat Analysis Report shows the TIE Enterprise Reputation severity score. If not set, the McAfee GTI file reputation fetched from the TIE server is displayed in the Threat Analysis Report.

Configure LDAP

The LDAP (Lightweight Directory Access Protocol) feature enables Advanced Threat Defense to configure a dedicated LDAP server for user authentication. A separate server for user authentication facilitates a secured and centralized authentication system. It provides a robust and secure credential authentication and management system for various types of Advanced Threat Defense users. Also, configuring a dedicated LDAP server helps in avoiding data replication (at multiple hosts) and thus increasing data consistency.

LDAP authentication is applicable only to users with *Administrator* role enabled in Advanced Threat Defense. For non-administrative users like *nsp, mwg, atdadmin,* and *tie*, authentication using an LDAP server is not supported. Authentication for these users is made using the Advanced Threat Defense database.

The following user accounts (data) must be created on the LDAP server. Accounts created on the LDAP server must be the same as on the Advanced Threat Defense appliance.

- **Base Distinguished Name (BaseDN):** Create a specific BaseDN for Advanced Threat Defense users. BaseDN acts as a root node under which all the Advanced Threat Defense users are added.
- **Admin Credentials:** To enable the LDAP option, credentials (user name and password) of the *Administrator* user must be provided in the Advanced Threat Defense user interface. If the, *Administrator* user is not present, users must create the same in the LDAP server (directory).
- **User creation:** Create users manually on an LDAP server. The following table contains the list of users needed.

Table 6-1 Users in LDAP server

User_Name	Type	Service used
admin	User Interface	UI, SFTP
nsp	User Interface	UI, SFTP
atdadmin	User Interface	UI, SFTP
mwg	User Interface	UI, SFTP
meg	User Interface	UI, SFTP
vnsp	User Interface	UI, SFTP
nonadmin	User Interface	UI, SFTP
tie	User Interface	UI, SFTP
cliadmin	System	CLI

During the LDAP logon, username must match the username created locally in the Advanced Threat Defense database. Username is case sensitive.

Task

1. Select **Manage** | **Configuration** | **LDAP**.
2. Select the **Enable LDAP** checkbox.
3. Enter these details.

Option name	Definition
Username (DN)	Enter a user name for Advanced Threat Defense to use to access the LDAP server. The user name must be specified in the DN format. For example, CN=root,OU=atd, DC=myhost and DC=com.
Password	Enter the password.
Authentication Method	Select the authentication method to be used to communicate with the LDAP server.
IP Address	Specify the IP address of the LDAP server.
Port Number	This field is populated automatically based on the selected authentication method. The default port number is 389 for Simple authentication and 636 for SSL authentication. Users can manually configure a different port number.
Base DN	Specify the name of the domain in the LDAP server database where the search is to be performed. The name must be in DN format. For example, OU=atd, DC=myhost and DC=com.
LDAP Scope	Specify the search scope in the LDAP server. It has the following three options: • **Subtree**: The complete subtree of the **BaseDN** is searched. • **Onelevel**: One level below the **BaseDN** is searched. • **Base**: The base of the **BaseDN** is searched.
Login Attribute	Specify the attribute of the field to be searched in the LDAP server database. For example, in case of OpenLDAP, login attribute can be `uid` and in case of Microsoft Active Directory, it can be `sAMAccountName`.

4. Click the **Test Connection** tab. When the **LDAP Test connection successful** message appears, click **OK**.
5. Click the **Submit** tab. The **LDAP configuration saved successfully** message appears. The LDAP server configuration is now complete.

> Select **Enable Fallback** in case the configured LDAP server is not reachable and the authentication channel needs to be routed to Advanced Threat Defense local database. For *cliadmin* users, **Enable Fallback** is always enabled.

> LDAP authentication is used for SFTP communication with Advanced Threat Defense. The fallback feature is not supported when SFTP communication is used.

Configure SNMP setting

The SNMP service allows users to obtain integral values for the following quantifiable attributes of the Advanced Threat Defense components. This information enables users to manage Advanced Threat Defense resources in an efficient manner.

- CPU Utilization
- Memory Utilization
- HDD System Space Utilization
- HDD Data Space Utilization
- Interface Counter
- System Temperature
- Number of samples in waiting queue
- Number of samples under analysis

You issue `snmpget` command in the command prompt or any MIB browser to retrieve the numeric value for the above mentioned attributes.

You can also configure SNMP services to receive *SNMP TRAPS* for the following attributes. *SNMP TRAPS* are alert messages that notify users that the integral values of the following attributes has reached or exceeded the user-defined limit for that attribute. Traps are sent every 60 seconds if the integral value exceeds the configured threshold value for CPU Utilization and Memory Utilization.

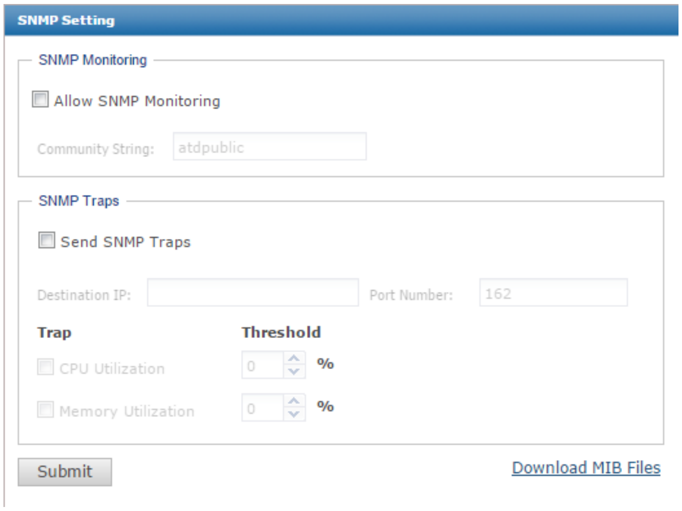
- CPU Utilization
- Memory Utilization

Minimum threshold level supported is 30%. Maximum threshold level supported is 90%. By default, the threshold percentage displayed under **SNMP Setting** page is 75%.

> **CPU Utilization** field appearing in the **SNMP Setting** page is different from **CPU Load** featuring under **System Health** under **Dashboard** tab.

Task

1 Select **Manage** | **Configuration** | **SNMP Setting.**



SNMP Setting

SNMP Monitoring

□ Allow SNMP Monitoring

Community String: atdpublic

SNMP Traps

□ Send SNMP Traps

Destination IP: Port Number: 162

Trap	Threshold
□ CPU Utilization	0 %
□ Memory Utilization	0 %

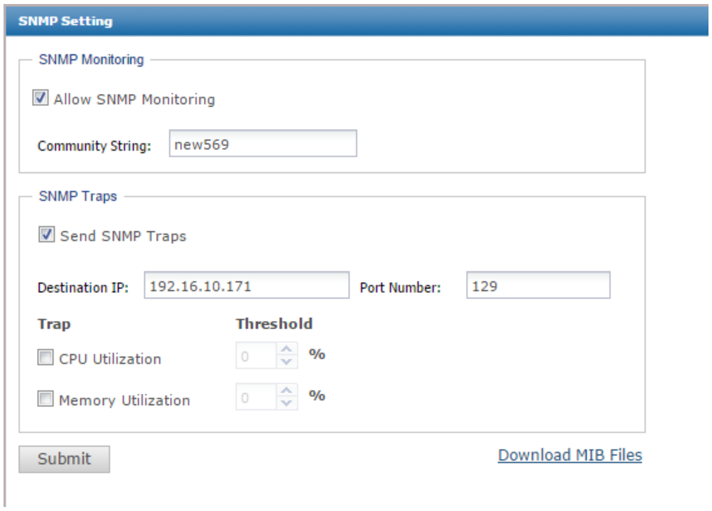
2 In the **SNMP Monitoring** area, select **Allow SNMP Monitoring**.

> You can modify the **SNMP Community String**. By default it is set as **atdpublic**.

3 In the **SNMP Traps** area, make these selections and entries.

- Select **Send SNMP Traps**.
- Enter the IP address of your local machine in the **Destination IP** field.

- Enter a SNMP trap port. By default, this is set as **162**.
- Under **Trap**, select the **Threshold** percentage for the required attributes.



SNMP Setting

SNMP Monitoring

☑ Allow SNMP Monitoring

Community String: new569

SNMP Traps

☑ Send SNMP Traps

Destination IP: 192.16.10.171 Port Number: 129

Trap	Threshold
□ CPU Utilization	0 %
□ Memory Utilization	0 %

4 Click **Submit**. The **SNMP setting has been saved successfully** message is displayed.

> All the associated MIB files of respective entities or objects can be downloaded locally by clicking on **Download MIB Files**.

Integration with McAfee Next Generation Firewall

McAfee Next Generation Firewall integrates security features with high availability and manageability. It integrates application control, Intrusion Prevention System (IPS), and evasion prevention into a single, affordable solution. Following steps should be performed by McAfee Next Generation Firewall customer in order to integrate McAfee Next Generation Firewall with McAfee Advanced Threat Defense:

1 Create a user called “ngfw” on Advanced Threat Defense after logging into Advanced Threat Defense as "admin". This user has the same privileges as the "nsp" user.

2 Restart amas from the CLI.

3 Use "ngfw" user on SCM to make REST API calls.

> There is no change to the existing SOFA protocol for file submission. Since a user called “ngfw” exists, all file submissions via the SOFA channel is assumed to be from McAfee NGFW appliances.

Configure proxy servers for Internet connectivity

Advanced Threat Defense connects to different proxy servers for Internet connectivity. Based on the source of the traffic, Advanced Threat Defense determines the proxy server on which the Internet access requests from the traffic have to be routed.

These proxy servers can be configured on Advanced Threat Defense to handle Internet access requests:

- **GTI HTTP Proxy** — This setting is relevant for those analyzer profiles which have *GTI Reputation* enabled in their Analyzing Options. Advanced Threat Defense sends a query to a McAfee GTI server to fetch McAfee GTI score for the suspicious file being analyzed. If the customer network is protected under proxy, specify the proxy server details here so that the McAfee GTI queries can be sent out.
- **Malware Site Proxy** — This setting is applicable when samples being analyzed at analyzer VMs request Internet access. The proxy server specified under **Malware Site Proxy** handles the request. Because the traffic from an analyzer VM might be malicious, you might want to segregate this traffic from your production network.

Tasks

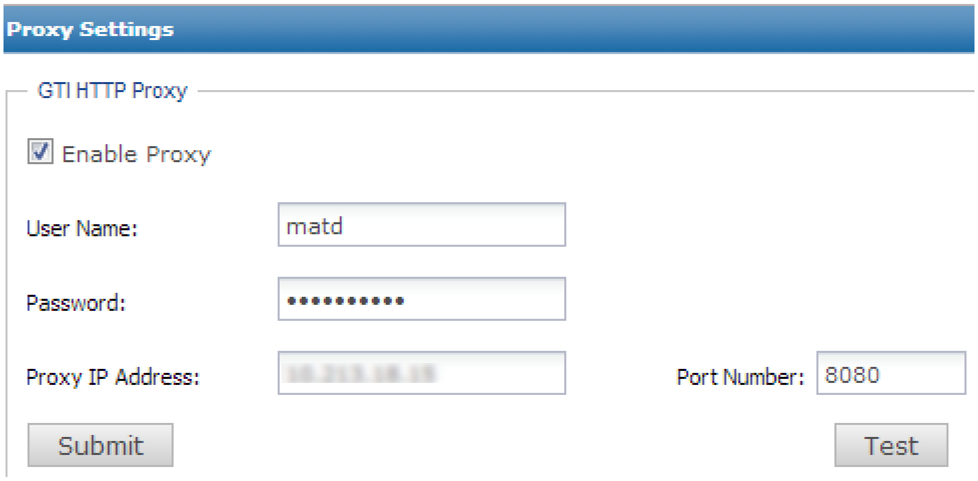
- *Specify Proxy Settings for Global Threat Intelligence traffic* on page 255
- *Specify Malware Site Proxy Settings for Malware traffic* on page 256

Specify Proxy Settings for Global Threat Intelligence traffic

Task

1 Select **Manage** | **Configuration** | **Proxy Settings.**

On the **Proxy Settings** page, **GTI HTTP Proxy** section is displayed.



Proxy Settings

GTI HTTP Proxy

☑ Enable Proxy

User Name: matd

Password: ••••••••••

Proxy IP Address: [redacted]

Port Number: 8080

Figure 6-5 **Proxy Settings** **page**

To enable this option, the **GTI File Reputation** option under **Analyze Options** must be enabled.

2 In the **GTI HTTP Proxy** area, enter the appropriate information in the respective fields.

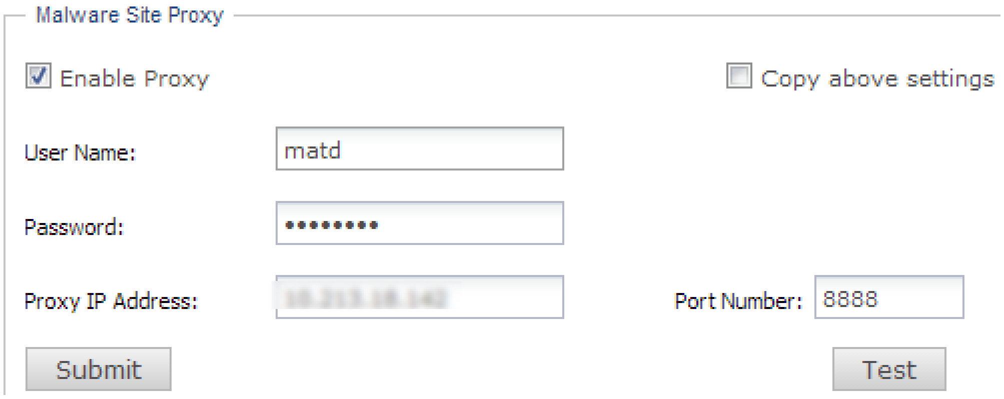
Option name	Definition
Enable Proxy	Select to connect Advanced Threat Defense to a proxy server for Internet connectivity.
User Name	Enter the user name that Advanced Threat Defense uses for the proxied Internet connection.
Password	Enter the corresponding password.
Proxy IP Address	Enter the IPv4 address of the proxy server.
Port Number	Enter the port number on which the proxy server is listening for incoming connections.
Test	Click to verify if Advanced Threat Defense is able to reach the configured HTTP proxy server over the specified port.
Submit	Click to save the proxy settings in the database. Make sure that the test connection is successful before you click **Submit**.

Specify Malware Site Proxy Settings for Malware traffic

Task

1 Select **Manage** | **Configuration** | **Proxy Settings.**

On the **Proxy Settings** page, **Malware Site Proxy** section is displayed.



Malware Site Proxy

☑ Enable Proxy

□ Copy above settings

User Name: matd

Password: ••••••••

Proxy IP Address: [redacted]

Port Number: 8888

Figure 6-6 Proxy Settings page

2 In the Malware Site Proxy area, enter the appropriate information in the respective fields.

Option name	Definition
Enable Proxy	Select to connect Advanced Threat Defense to a proxy server for Internet connectivity.
User Name	Enter the user name that Advanced Threat Defense uses for the proxied Internet connection.
Password	Enter the corresponding password.
Proxy IP Address	Enter the IPv4 address of the proxy server.
Port Number	Enter the port number on which the proxy server is listening for incoming connections.
Copy above settings	Select to replicate the proxy settings made in the **GTI HTTP Proxy Settings** section.
Test	Click to verify if Advanced Threat Defense is able to reach the configured HTTP proxy server over the specified port.
Submit	Click to save the proxy settings in the database. Make sure that the test connection is successful before you click **Submit.**

Configure Syslog Setting

The syslog mechanism transfers the analysis result events over the syslog channel to Security Information and Event Management (SIEM) like McAfee Enterprise Security Manager (McAfee ESM). This is done for all the files analyzed by Advanced Threat Defense. You can configure an external syslog server to which the following information is sent:

- Analysis Results
- CPU Utilization
- Memory Utilization
- HDD Utilization
- Interface Status
- User Login/Logout
- Audit Log
- HTTPS Session Log

Once the user-defined threshold limit exceeds for CPU Utilization, Memory Utilization and HDD Utilization, syslog events are generated and sent to SIEM receiver. Minimum threshold level supported is 30%. Maximum threshold level supported is 90%. By default, the threshold percentage displayed under **Syslog Setting** page is 75%.

Whenever the interface link goes down or comes up, syslog events are generated and sent to SIEM receiver.

Analysis results and logon/logoff events are sent to the SIEM receiver.

After syslog events are generated and sent to SIEM receiver, the information are parsed and sent to ESM. The summary is then displayed on the ESM user interface.

The SIEM receiver and ESM can be on separate appliances or can be together in a virtual environment.

Task

1 Select **Manage** | **Configuration** | **Syslog Setting.**

2 In the **Off-box system log** area, make these selections and entries.

- Select **Enable**
- **IP Address**— IP address of the syslog server
- **Port**— Listening port number for the syslog server (default is 514)
- **Protocol**— Select a protocol from the drop-down list. Default protocol used for Audit function is TCP/TLS Encryption.
- **Certificate File**— Upload a valid certificate in PEM/CRT format using **Browse** button for **Audit** function

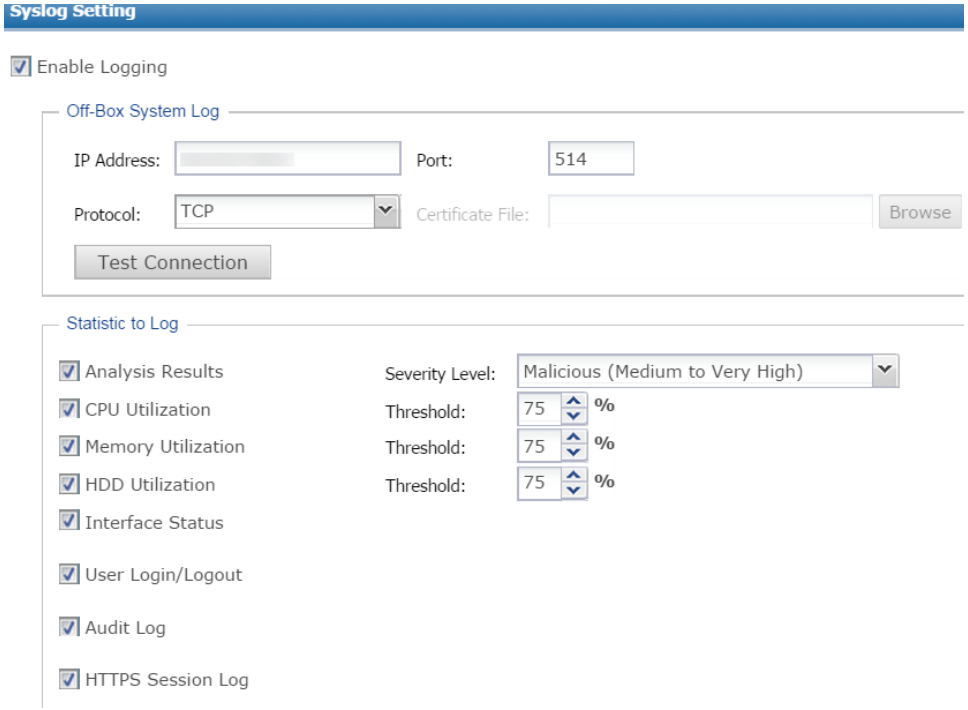
> In non-CC mode, any valid certificate along with key can be uploaded as no check on key length or signature algorithm is performed. However, in CC mode, key length should be 2048 and above and signature algorithm should be minimum SHA256 with RSA Encryption. Default listening port for **Audit** function is 6514 and protocol used for same is **TCP/TLS Encryption**. Web server supports TLS1.0,TLS1.1 and TLS1.2 protocols.

3 Click **Test Connection**. When the "Test connection successful" message appears, click **OK**.

> If we select **UDP** as **Protocol** from the drop-down list then **Test Connection** tab is disabled as UDP uses a simple connectionless transmission model rendering the connection status, unverifiable.

4 In the **Statistic to Log** area, make these selections and entries as per requirement.

- Select **Analysis Results**.
- Select a level from the **Severity Level** drop-down list.
- Select **CPU Utilization** and specify Threshold level in the respective **Threshold** drop-down.
- Select **Memory Utilization** and specify Threshold level in the respective **Threshold** drop-down.
- Select **HDD Utilization** and specify Threshold level in the respective **Threshold** drop-down.
- Select **Interface Status** to receive information regarding interface link status.
- If you want to store the logon/logoff information with a time stamp, select **User Login/Logout**.
- Select **Audit Log** to view logs for administrative actions performed on Advanced Threat Defense. **Audit Log** is selected by default.
- Select **HTTPS Session Log** to view logs for every session established or terminated.



Syslog Setting

☑ Enable Logging

Off-Box System Log

IP Address: [redacted]

Port: 514

Protocol: TCP

Certificate File:

Statistic to Log

☑ Analysis Results — Severity Level: Malicious (Medium to Very High)

☑ CPU Utilization — Threshold: 75 %

☑ Memory Utilization — Threshold: 75 %

☑ HDD Utilization — Threshold: 75 %

☑ Interface Status

☑ User Login/Logout

☑ Audit Log

☑ HTTPS Session Log

5 Click **Submit**. The **Off-box syslog setting was submitted successfully** message is displayed.

Sample for **Analysis Results** log events that is displayed in ESM:

```
2015-03-26T01:55:02. localhost ATD2ESM[13207]: {"Summary": { "Event_Type": "ATD
File Report","MISversion": "3.4.4.2.43772","SUMversion":
"3.4.4.2.43772","OSversion": "win7sp1x64","fileId": "Not Available","Parent MD5":
"Not Available","ATD IP": "10.213.248.17","Src IP": "10.213.248.69","Dst IP":
"10.213.248.107","TaskId": "37","JobId": "37","JSONversion":
"1.001.0718","hasDynamicAnalysis": "true","Subject": {"Name": " http://
10.213.248.107/Apoorv/samples/automation_samples/vtest64.exe","Type": "PE32+
executable (console) x86-64","md5": "6AF8F4E3601156A59F050AAB4FAB5153","sha-1":
"11BBBA1E7B39E1E193C6740B61F2A32E30ADD01A","size": "56832","Timestamp": "2014-12-15
11:24:12","parent_archive": "Not Available"},"Selectors": [{"Engine":
"Sandbox","MalwareName": "Malware.Dynamic","Severity": "5"}],"Verdict":
{"Severity": "5","Description": "Sample is malicious"},"Stats": [{"ID":
"0","Category": "Persistence, Installation Boot Survival","Severity": "5"},{"ID":
"1","Category": "Hiding, Camouflage, Stealthiness, Detection and Removal
Protection","Severity": "0"},{"ID": "2","Category": "Security Solution / Mechanism
bypass, termination and removal, Anti Debugging, VM Detection","Severity": "5"},
{"ID": "3","Category": "Spreading","Severity": "2"},{"ID": "4","Category":
"Exploiting, Shellcode","Severity": "0"},{"ID": "5","Category":
"Networking","Severity": "3"},{"ID": "6","Category": "Data spying, Sniffing,
Keylogging, Ebanking Fraud","Severity": "4"}],"Behavior": ["Created content under
Windows system directory","Deleted AV auto-run registry key","Created a socket
bound to a specific service provider and listen to an open port","Installed low
level keyboard hook procedure","Deleted a key from auto-run registry
entry","Altered auto-run registry entry that executed at next Windows boot"]}}
```

Sample for **CPU Utilization** log events that is displayed in ESM:

```
Dec 8 12:50:02 ATD-3000 ATD2ESM[22415]: {"CPU Alert": {"CPU Usage":46.0, "CPU
Threshold":30.0}}
```

Sample for **Memory Utilization** log events that is displayed in ESM:

```
Dec 8 13:45:04 ATD-3000 ATD2ESM[2922]: {"Memory Alert": {"Memory Usage":46.4,
"Memory Threshold":30.0}}
```

Sample for **HDD Utilization** log events that is displayed in ESM:

```
Dec 8 12:50:02 ATD-3000 ATD2ESM[22415]: {"Disk Alert": {"Data Disk Usage":42.7,
"Disk Usage Threshold":30.0}}
```

```
Dec 8 12:50:02 ATD-3000 ATD2ESM[22415]: {"Disk Alert": {"System Disk Usage":52.3,
"Disk Usage Threshold":30.0}}
```

Sample for **Interface Status** log events that is displayed in ESM: Interface can either be eth0 / eth1 / eth2 / eth3 depending on the configuration and the Interface Status shows either interface is up or down

```
Dec 8 17:20:03 ATD-3000 ATD2ESM[16594]: {"Link Alert": {"eth0 Link": "Down"}}
```

```
Dec 8 17:55:03 ATD-3000 ATD2ESM[17099]: {"Link Alert": {"eth1 Link": "Up"}}
```

Sample for **User Login/Logout** log events that is displayed in ESM:

```
<181>Aug 20 00:33:42 ATD-3000 MATD-LOG[6902]: {"Action": "Successful user login",
"User": "meg", "UserID": "5", "Timestamp": "2014-08-20 07:33:42", "Client":
"10.213.248.120"}
```

Sample for **Audit Log** events that is displayed in ESM:

```
2015-03-26T01:55:02.783269+05:30 MATD2U0XX-243 ATD2ESM[16638]:
{"Type":"Audit","MsgId":"M-CC-01-0","Result":"Success","User":"admin","Category":"A
dmin","Client":"10.70.168.72","Action":"Common Criteria
Modification","Description":"Common Criteria mode is saved successfully"}
```

```
2015-03-17T22:23:15.979017+05:30 MATD2U0XX-243 login: {"Type":"Audit",
"MsgId":"C-LO-01-0", "Result":"Success", "User":"CLI", "Category":"Admin",
"Client":"", "Action":"CLI Login", "Description":"Login Success (tty1)"}
```

Tasks

- *View Syslog log* on page 261
- *View Audit Log* on page 261

View Syslog log

As per the selections made in the **Syslog Setting** page, McAfee Advanced Threat Defense starts logging syslog events taking place within the Advanced Threat Defense. Simultaneously, it prints the related logs, which you can view in the Advanced Threat Defense web application. You can use this information for troubleshooting purposes.

- After you click **Submit** in the **Syslog Setting** page, select **Manage** | **Logs** | **Syslog** to view the log entries.

  A maximum of 1000 events are displayed in Advanced Threat Defense user interface with latest events at the bottom. More events are available in the configured syslog server. You cannot print or export the log entries.

View Audit Log

When you configure audit function by checking on the **Audit Log** using **Syslog Setting** page, McAfee Advanced Threat Defense starts logging the administrative actions performed within the Advanced Threat Defense. Through these log entries, you can view what is happening as the administrative actions, for example, configuration change, session establishment/session termination and so on are performed. These log entries are displayed in a tabular form. You can use this information for troubleshooting purposes.

- After you click **Submit** in the **Syslog Setting** page, select **Manage** | **Logs** | **Audit Log** to view the log entries.

  A maximum of 1000 events are displayed in Advanced Threat Defense user interface with latest events at the top. More events are available in the configured syslog server. You cannot print or export the log entries.

Configure DNS setting

When being executed, some files might send DNS queries to resolve names. Mostly, such queries are an attempt by malware to determine if they are being run in a sandbox environment. If the DNS query fails, the file might take an alternate path. When Advanced Threat Defense dynamically analyzes such a file, you might want to provide a proxy DNS service in order to bring out the actual behavior of the file.

Task

1. Select **Manage** | **Configuration** | **DNS Setting.**

   The **DNS Setting** page is displayed.

2. Enter the appropriate information in the respective fields.

Option name	Definition
Domain	Enter the Active Directory domain name, for example, McAfee.com.
Preferred DNS Server	Enter the IPv4 address of the primary DNS proxy server. The DNS queries from analyzer VMs are come to this DNS server.
Alternate DNS Server	Enter the IPv4 address of the secondary DNS proxy server. If the analyzer VM is unable to reach the primary DNS server, the DNS queries come to the secondary DNS server.
Test	Click verify if Advanced Threat Defense is able to reach either the preferred or the alternate DNS server.
Submit	Click to save the configuration in the database. Make sure that the test connection is successful before you click **Submit.**

ℹ After any DNS configuration change, use CLI command `amas restart` to restart the amas services.

Configure date and time settings

Before you begin

- You need *admin user* privileges to view or set the date and time settings.
- If you plan to use domain names of Network Security Protocol servers, make sure you have configured the DNS servers correctly in Advanced Threat Defense.

You can set the date and time on the Advanced Threat Defense Appliance as per your requirement in the **Date and Time Settings** page. Advanced Threat Defense uses the date and time that you configure for all its functional and display purposes. The date and time in the Advanced Threat Defense web application user interfaces, reports, log files, and CLI are all as per the date and time that you specify. For example, the timestamp in the Analysis Status and Analysis Results pages are as per the date and time that you configure.

You can either manually specify the date and time or configure Network Time Protocol (NTP) servers as the time source for Advanced Threat Defense. If you specify NTP servers, you can configure up to 3 Network Time Protocol (NTP) servers. In this case, Advanced Threat Defense acts as an NTP client and synchronizes with the highest priority NTP server that is available.

- By default, synchronization with NTP servers is enabled in Advanced Threat Defense. Also, `pool.ntp.org` is configured as the default NTP server. The default time zone is Pacific Standard Time (UTC-8).
- When you upgrade from a previous version without selecting the **Reset Database** option, the date and time settings from the previously installed version are preserved. If you upgrade with the **Reset Database** option selected, the default date and time settings as described above are set.
- At any point in time, there must be at least one valid NTP server specified in the **Date and Time Settings** page of Advanced Threat Defense. You can add, edit, or delete the list of NTP servers specified in Advanced Threat Defense.

- Based on the access available to Advanced Threat Defense, you can specify public NTP servers or the ones locally on your network.
- You can specify the domain name or the IPv4 address of NTP servers. If you specify the domain names, then you must have configured DNS settings in Advanced Threat Defense.

> If you specify public NTP servers, then using the domain names instead of IP addresses is recommended. The domain of a public NTP server might resolve to different IP addresses based on various factors.

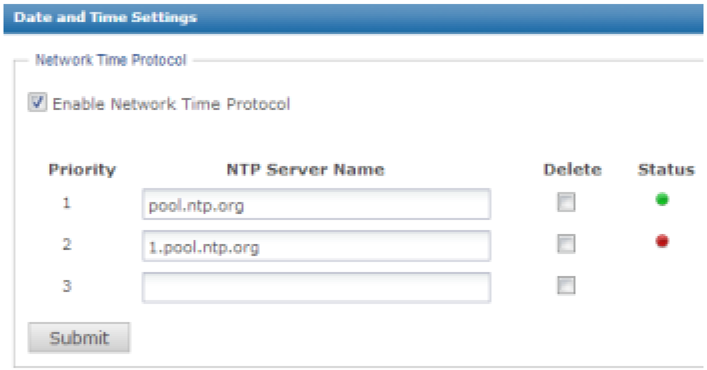
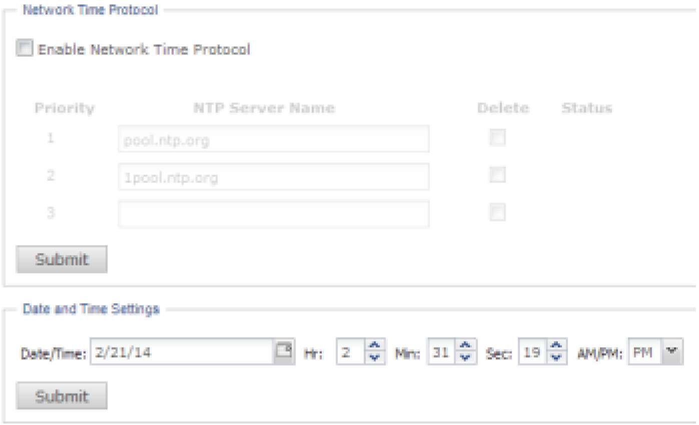
- Whether you enable NTP server synchronization or manually set the date and time, you must select the required time zone in the **Date and Time Settings** page. If you configure an NTP server, Advanced Threat Defense considers only the date and time from the NTP server. But for the time zone, it relies on what is specified in the Date and Time Settings page.
- The date and time on a Advanced Threat Defense client has no impact on the timestamps that are displayed. Consider that the current time on the Advanced Threat Defense Appliance is 10 am PST (UTC-8). Regardless of the time zone from which you access this Advanced Threat Defense Appliance, all the timestamps are displayed in PST only. That is, the timestamps are not converted based on a client's date and time.
- When the current date and time settings are changed, the timestamp for all the older records are also changed accordingly. Consider that the current time zone is PST (UTC-8) and you change it to Japan Standard Time (UTC+9). Then the timestamp for the older records are all converted as per Japan Standard Time (JST). For example, if the timestamp displayed for a record in the **Analysis Status** page was 0100 hours (1 am) PST before you changed the time zone. After you change the time zone to JST, the timestamp for the same record is 1800 hours JST.
- The date and time settings of all the analyzer VMs are immediately synchronized to the date and time on the Advanced Threat Defense Appliance.

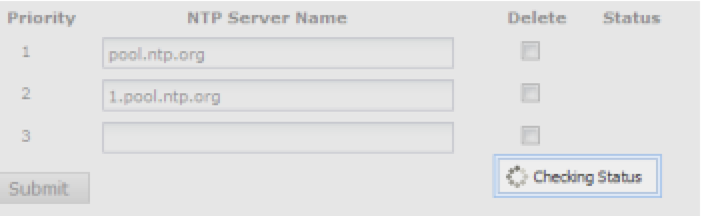
Task

1 Select **Manage** | **Configuration** | **Date and Time Settings.**

The **Date and Time Settings** page is displayed.

2 Enter the appropriate information in the respective fields and click **Submit** in the affected sections separately.

Option name	Definition
Enable Network Time Protocol	Select if you want Advanced Threat Defense to act as an NTP client. By default this is selected. To manually set the time for Advanced Threat Defense, deselect this option.
Priority	This is the order of priority assigned to the NTP servers. At the scheduled interval, Advanced Threat Defense attempts to synchronize with the first NTP server. If not available, it attempts to synchronize with the second and then the third.
NTP Server Name	Specify the domain name or IPv4 addresses of the NTP servers in the order of priority that Advanced Threat Defense should synchronize with. If you enter domain names, make sure you have configured the DNS settings properly. At any point in time, there must be at least one reachable NTP server configured.
Delete	Select if you want to remove an NTP server from the list.
Status	Indicates whether a particular NTP server is reachable or not. Green indicates the server is reachable and red indicates that the server is not reachable.  Date and Time Settings Network Time Protocol ☑ Enable Network Time Protocol Priority / NTP Server Name / Delete / Status 1 / pool.ntp.org / □ / 🟢 2 / 1.pool.ntp.org / □ / 🔴 3 / / □ Submit
Date/Time	To manually specify the date and time for Advanced Threat Defense, deselect **Enable Network Time Protocol** and click **Submit** under **Network Time Protocol**. Specify the date and time in the corresponding fields and then click **Submit** under **Date and Time Settings**.  Network Time Protocol □ Enable Network Time Protocol Priority / NTP Server Name / Delete / Status 1 / pool.ntp.org / □ 2 / 1pool.ntp.org / □ 3 / / □ Submit Date and Time Settings Date/Time: 2/21/14 Hr: 2 Min: 31 Sec: 19 AM/PM: PM Submit

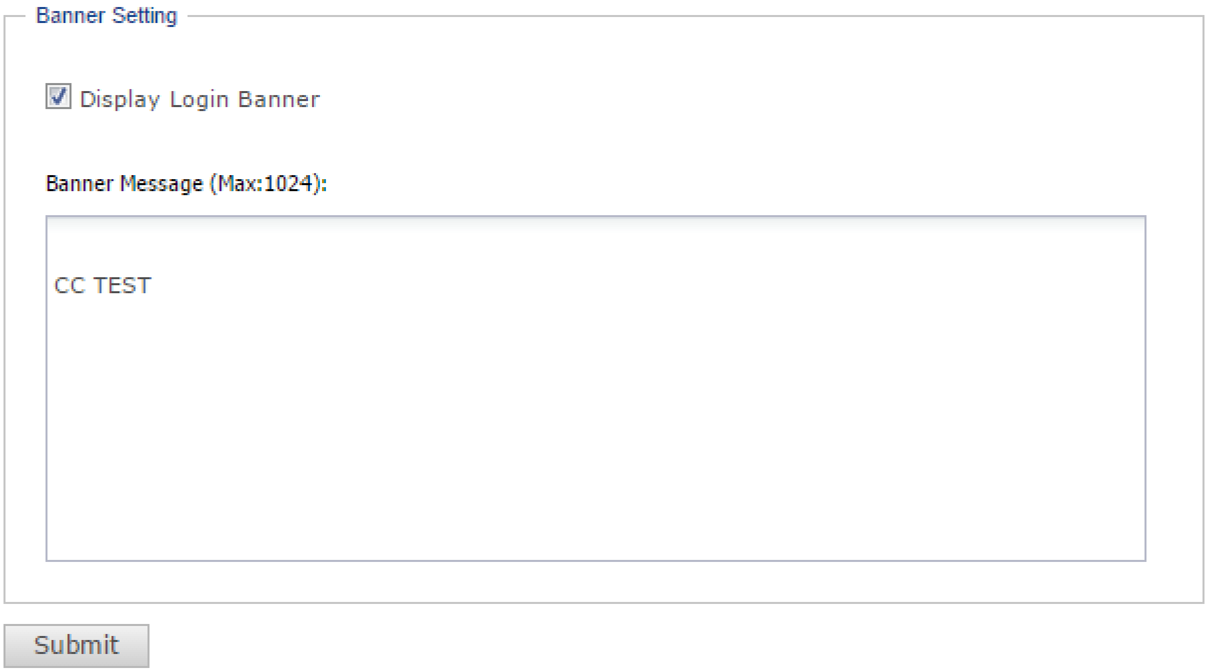
Option name	Definition
Select Time-zone	Select the required time zone from the list and click **Submit** under **Time-zone Setting**. The default time zone is Pacific Time.
Submit	Implements the changes that you made in the corresponding sections of the **Date and time settings** page and also saves them in the database. After you click **Submit** for Network Time Protocol, a success message is displayed. If you click **OK** for this message, Advanced Threat Defense checks if it can reach the specified NTP servers and updates the **Status** accordingly for each NTP server.  Priority NTP Server Name Delete Status 1 pool.ntp.org □ 2 1.pool.ntp.org □ 3 □ Submit Checking Status You must click the **Submit** separately for affected sections. For example, if you make changes to the list of NTP servers and also change the time zone, you must click **Submit** under **Network Time Protocol** and **Submit** under **Time-zone Setting** separately.

Add a Advanced Threat Defense login banner

The login banner page enables you to upload customized text on Advanced Threat Defense logon page.

To upload a login banner, do the following:

1. Click **Manage** | **Configuration** | **Login Banner** and select **Display Banner**.
2. Write the desired login message.



☑ Display Login Banner

Banner Message (Max:1024):

CC TEST

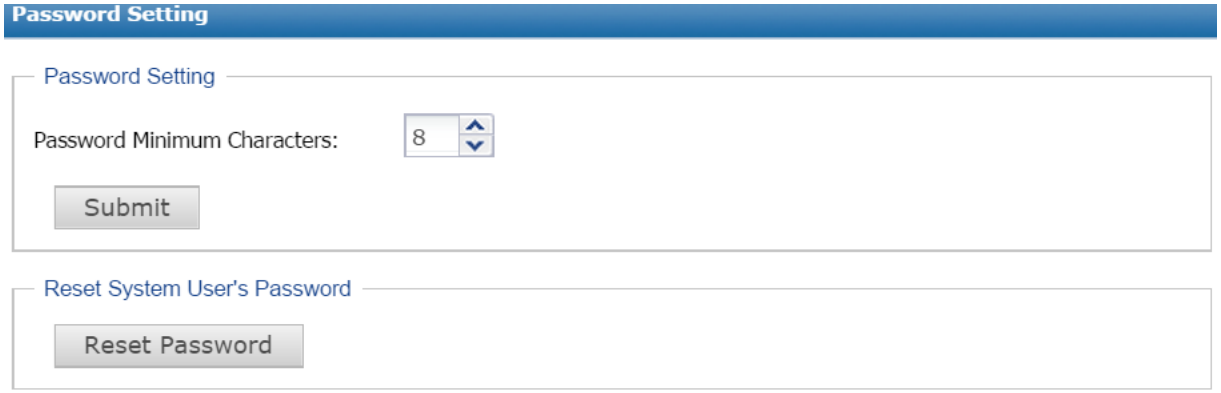
3. Click **Submit** to save changes.

> Maximum number of characters allowed for banner message is 1024. Only ASCII character set is allowed.

Set minimum number of characters for password

Using **Password Setting** page, user can set minimum number of characters to be used while creating password to log on to Advanced Threat Defense. The default password length is 8 characters. The same password constraints apply for console access and CLI access.

Use **Reset Password** tab to reset password for CLI user and troubleshooting password (nobrk1n) to default.



Configure Telemetry

The Telemetry feature allows Advanced Threat Defense to collect data about malware and subsequently send the respective reports to McAfee GTI server. The feature also allows Advanced Threat Defense to collect data about the Advanced Threat Defense Appliance.

Broadly, the data captured by Advanced Threat Defense can be classified under the following two categories:

- Telemetry data for McAfee GTI/ McAfee Labs

  McAfee Labs requires analysis results from Advanced Threat Defense, as telemetry, to update their databases in order to categorize the samples/malware which were analyzed by Advanced Threat Defense. The telemetry data contain various information related to the samples analyzed. The list of data collected for McAfee labs is as follows:

  - SHA-1 of sample
  - SHA-256 of sample
  - MD5 hash value of sample
  - Advanced Threat Defense detection score
  - Digital signature data from sample
  - Parent metadata corresponding to dropped files
  - Advanced Threat Defense product information
  - Advanced Threat Defense analyzing option scores
  - URL visited by file
  - IPv4 address visited by file
  - Product version that the sample belongs to
  - Publisher name of the sample
  - Product name that the sample belongs to
  - File version of the sample, OS name, and OS version on which the file was found on

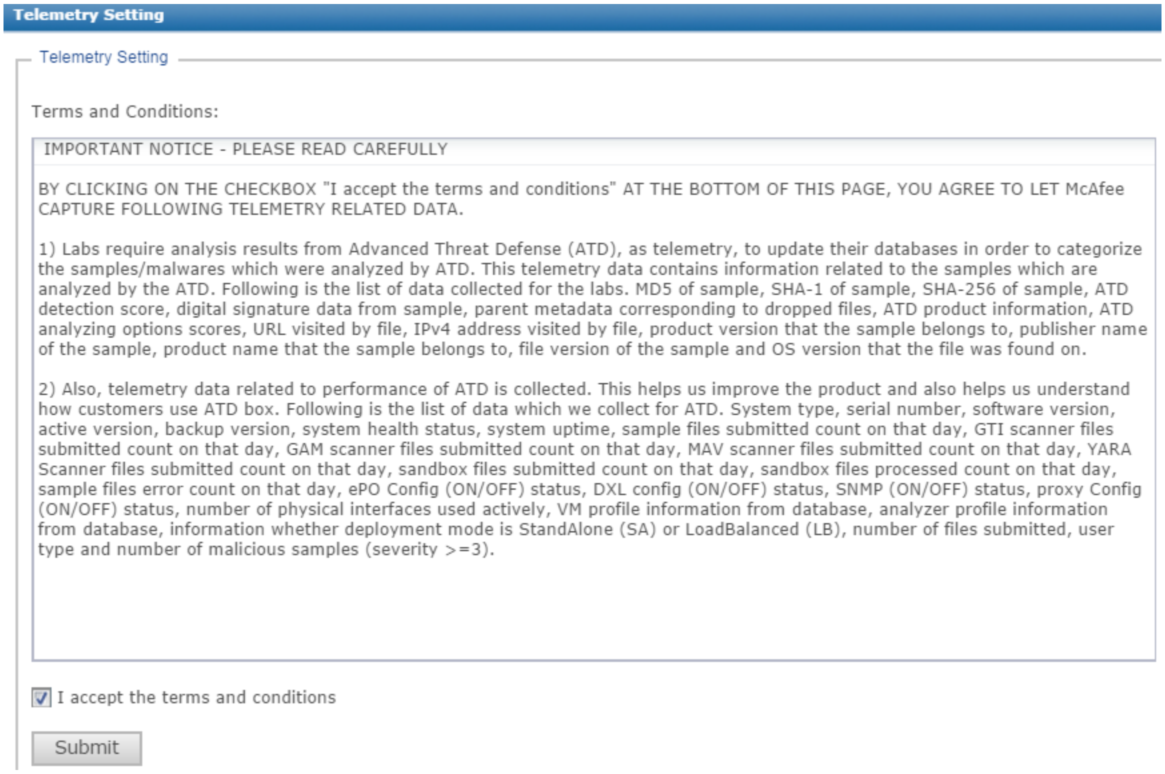
- Telemetry data for the Advanced Threat Defense Appliance to be used by Advanced Threat Defense

Telemetry data related to the Advanced Threat Defense Appliance are collected. This helps McAfee to improve Advanced Threat Defense and understand how the Advanced Threat Defense Appliance is used. The list of system data collected for Advanced Threat Defense is as follows:

- Serial number
- Software version
- Active version
- Advanced Threat Defense Appliance backup version
- System health status
- System uptime
- Count of sample files submitted
- Count of McAfee GTI scanner files submitted
- Count of GAM scanner files submitted
- Count of AV scanner files submitted
- Count of YARA scanner files submitted
- Count of Sandbox files submitted
- Count of Sandbox files processed
- Count of sample files errors
- McAfee ePO configuration status (ON/OFF)
- DXL configuration status (ON/OFF)
- SNMP status (ON/OFF)
- Proxy configuration status (ON/OFF)
- Number of physical interfaces configured
- VM profile information
- Analyzer profile information
- Information whether deployment mode is StandAlone (SA) or LoadBalanced (LB)
- Number of files submitted – user type and number of malicious samples (Severity>=3)

Task

1. Select **Manage** | **Configuration** | **Telemetry**.
2. Select **I accept the terms and conditions** at the bottom of the page.
3. Click **Submit**.



Terms and Conditions:

IMPORTANT NOTICE - PLEASE READ CAREFULLY

BY CLICKING ON THE CHECKBOX "I accept the terms and conditions" AT THE BOTTOM OF THIS PAGE, YOU AGREE TO LET McAfee CAPTURE FOLLOWING TELEMETRY RELATED DATA.

1) Labs require analysis results from Advanced Threat Defense (ATD), as telemetry, to update their databases in order to categorize the samples/malwares which were analyzed by ATD. This telemetry data contains information related to the samples which are analyzed by the ATD. Following is the list of data collected for the labs. MD5 of sample, SHA-1 of sample, SHA-256 of sample, ATD detection score, digital signature data from sample, parent metadata corresponding to dropped files, ATD product information, ATD analyzing options scores, URL visited by file, IPv4 address visited by file, product version that the sample belongs to, publisher name of the sample, product name that the sample belongs to, file version of the sample and OS version that the file was found on.

2) Also, telemetry data related to performance of ATD is collected. This helps us improve the product and also helps us understand how customers use ATD box. Following is the list of data which we collect for ATD. System type, serial number, software version, active version, backup version, system health status, system uptime, sample files submitted count on that day, GTI scanner files submitted count on that day, GAM scanner files submitted count on that day, MAV scanner files submitted count on that day, YARA Scanner files submitted count on that day, sandbox files submitted count on that day, sandbox files processed count on that day, sample files error count on that day, ePO Config (ON/OFF) status, DXL config (ON/OFF) status, SNMP (ON/OFF) status, proxy Config (ON/OFF) status, number of physical interfaces used actively, VM profile information from database, analyzer profile information from database, information whether deployment mode is StandAlone (SA) or LoadBalanced (LB), number of files submitted, user type and number of malicious samples (severity >=3).

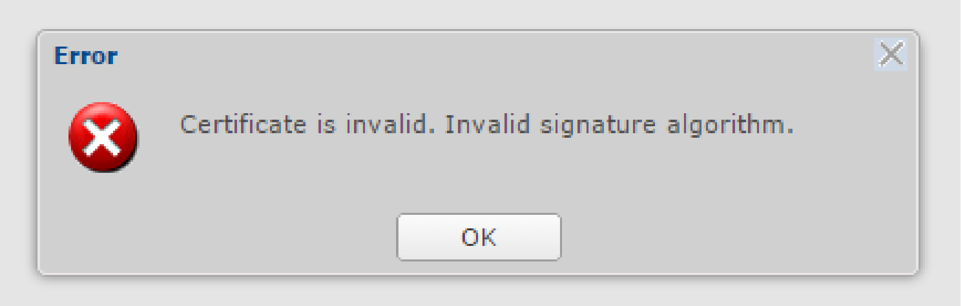
☑ I accept the terms and conditions

Upload Web Server certificate and CA certificate

Advanced Threat Defense allows customers to upload their own certificate for web server authentication. Follow the steps below to upload a certificate to Advanced Threat Defense.

1. Go to **Manage** | **Configuration** | **Web Certificate**.
2. In the **Web Certificate** section, upload a valid certificate along with the key in PEM format. The key length must be of 2048 characters and above and signature algorithm must be of minimum SHA256 standards with an RSA encryption. If the uploaded certificate does not contain key, **Certificate is invalid** message is displayed. Certificate uploaded for Syslog settings will be validated against the key length, signature algorithm, and expiry date.

3 In case of a problem with the uploaded certificate, an error message is displayed. An example of error message displayed incase of a certificate with invalid signature algorithm is shown below.



Certificate is invalid. Invalid signature algorithm.

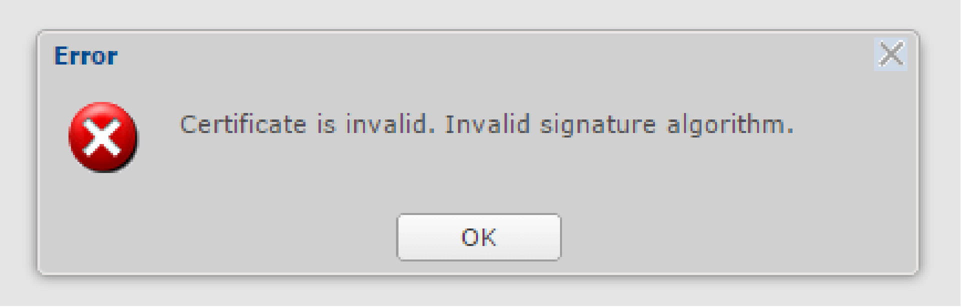
4 In case of no validation error, web server restarts and user needs to re-login to Advanced Threat Defense user interface.

Follow the steps below to upload a CA (Certificate Authority) certificate.

1 Go to **Manage** | **Configuration** | **Web Certificate**.

2 In the **CA Certificate** section, upload a valid CA certificate.

3 In case of a problem with the uploaded certificate, an error message is displayed. An example of error message displayed incase of a certificate with invalid signature algorithm is shown below.



Certificate is invalid. Invalid signature algorithm.

4 In case of no validation error, the specified CA certificate is uploaded successfully.

Configure maximum threshold wait time

Advanced Threat Defense allows you to configure the maximum wait time for analyzing samples received from McAfee Email Gateway. If the average analysis time of samples in Advanced Threat Defense is more than the threshold set, the samples submitted by McAfee Email Gateway are rejected.

Follow the steps below to configure the maximum wait time for analyzing samples received from McAfee Email.

1 Go to **Manage** | **ATD Configuration** | **Common Settings**.

2 In the **Performance Tuning** area, set the threshold wait time.

Enable Common Criteria setting

Follow below steps to enable **Common Criteria (CC)** mode in Advanced Threat Defense.

Task

1 Go to **Manage** | **Configuration** | **Common Criteria** and select **Enable Logging**. Enter the appropriate information in the respective fields.

2 In the **Off-box system log** area, enter the appropriate information in the respective fields.

Option name	Definition
IP Address	IP address of the syslog server.
Port	Listening port number for the syslog server. Default port is 6514.
Protocol	Select TCP/TLS Encryption from the drop-down list.
Certificate File	Upload a valid certificate in PEM/CRT format.

ⓘ Certificate uploaded for **Syslog Setting** is validated against key length, signature algorithm and expiry date. In case of a problem with certificate, Advanced Threat Defense displays an error message.

3 In the **Logging Features** area, make sure **Audit Log** is checked. By default **Audit Log** is enabled.

4 Click **Submit**.

5 Make sure FIPS mode is enabled. See set fips on page 363 for instructions on how to enable the FIPS mode. While in CC mode, FIPS mode must be enabled.

6 Make sure `http_redirect` is enabled. See http_redirect on page 353 command for instructions on how to enable the command. While in CC mode, `http_redirect` mode must be enabled.

7 Go to **Manage** | **Configuration** | **Common Criteria**, select **Enable Common Criteria Mode** and click **Submit**.

Audit function starts as Advanced Threat Defense boots up and stops with Advanced Threat Defense shutdown. The function restarts in the following two scenarios.

- Change in Syslog certificate
- Manual change in Date and Time information

ⓘ In Common Criteria (CC) mode, SSH access stops working and all opened SSH sessions are destroyed. Console access through console port or VGA port is available irrespective of CC/non-CC mode. SSH access is allowed in non-CC mode and can be managed from remote.

ⓘ On enabling CC mode, load-balancing feature gets disabled, hence load-balancing related configurations in Advanced Threat Defense user interface cannot be seen.

ⓘ CC Enabled Advanced Threat Defense can only be integrated with CC Enabled NSP build.

7 Update content on Advanced Threat Defense

You use the Advanced Threat Defense web application to upload contents to the Advanced Threat Defense Appliance. This section introduces you to the related contents and provides the procedures to upload the same to Advanced Threat Defense Appliance.

Contents

Uploading and managing content

Use these high-level steps to configure Advanced Threat Defense for uploading and managing content.

1. Select **Manage** | **Image & Software** | **Content Update**.
2. If you want your uploaded DAT versions to be updated automatically, select **Allow Automatic DAT Update** and click **Apply**. Your DAT file is updated with the latest version available, every 90 minutes.
3. In the **Uploaded Content** area, contents already uploaded are displayed under the relevant content tab heading.
4. Click required content on the **GAM-AV DATs**, **YARA Rules**, and **Detection Pkg** tabs to perform the following actions.
    - View the below listed information about uploaded content.
        - Feature - Specifies the name of the uploaded content
        - Engine - Specifies the name of the engine the content is applied to
        - DAT version - Specifies the version of the uploaded DAT
        - Engine Version - Specifies the version of the engine
        - Uploaded Date - Specifies the date and time of upload

- Status - Specifies whether the uploaded content is acting as **Current** or **Backup**. Content designated as **Current** is applied for malware detection.
- Action - Has two tabs, **Delete** and **Revert**. **Delete**, when used for the content serving as **Current**, disables the same and reverts **Backup** as **Current**. **Delete**, when used for content serving as **Backup** deletes the uploaded content. **Revert** is used to switch content designated as **Backup** to **Current**.

> Advanced Threat Defense allows you to import maximum two versions of YARA rules at any given time. The version uploaded later becomes **Current** by default, rendering the previous one as **Backup**. Rules defined in DAT file designated as **Current** are applied for malware detection.

- Upload the content. After clicking on the required tab, click **Browse** under **Manual Content Update** area and locate the content you want to upload. Refer the following links for more guidance on uploading the content.

Update DAT version for McAfee Gateway Anti-Malware and Anti-Virus on page 281

Import Custom Behavioral Rules and Custom Yara Scanner Rules on page 279

Upload Detection Package

Defining Custom Behavioral Rules

Custom Behavioral Rules is a set of YARA rules. YARA is a rule-based tool to identify and classify malware. Advanced Threat Defense enables you to use your own YARA rules to identify and classify malware. You can therefore import your own descriptions of malware into Advanced Threat Defense.

Custom Behavioral Rules also enable you to customize the detection capabilities of Advanced Threat Defense to suit your needs. For example, you can use Custom Behavioral Rules if you would like certain registry operations to be reported as a particular severity level rather than the default severity level assigned by Advanced Threat Defense. You can also write Custom Behavioral Rules to catch zero-day or near-zero-day malware. You can write your own Custom Behavioral Rules or use the YARA rules from a third party.

> In this section, the word sample refers to both files and URLs that have been submitted to Advanced Threat Defense for malware analysis.

You can store your Custom Behavioral Rules in a text file. You can name this file such that it enables you track modifications to your Custom Behavioral Rules set. You import this text file into Advanced Threat Defense through the web application user interface.

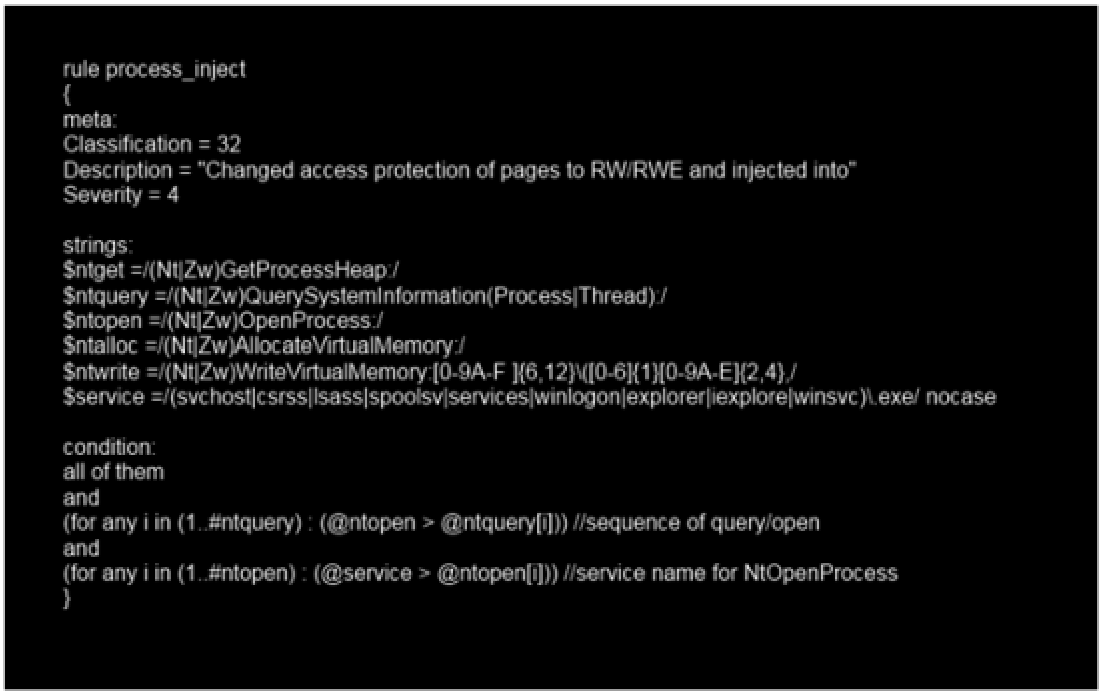
Assuming you have enabled all analyze options with custom YARA rules, Advanced Threat Defense processes the sample files and URLs in the following order of priority:

1. Local whitelist
2. Local blacklist
3. McAfee GTI
4. McAfee Gateway Anti-Malware Engine
5. McAfee Anti-Malware Engine
6. Custom Yara Scanner
7. Dynamic Analysis

8 Custom Behavioral Rules: These are user-managed YARA rules.

9 Internal YARA rules: These are internal YARA rules which are defined by McAfee and updated only during Advanced Threat Defense software upgrades, if necessary. You cannot view or download these rules.

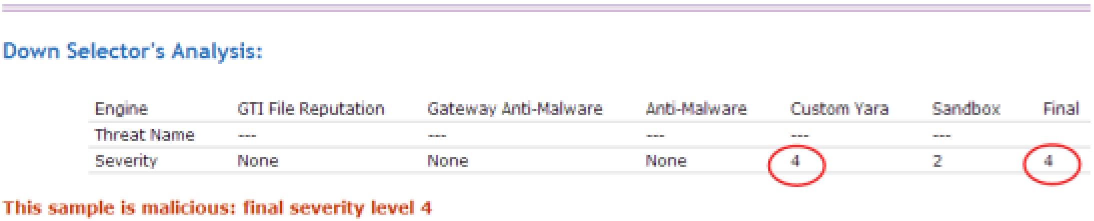
> McAfee Advanced Threat Defense checks a sample against YARA rules only if the sample is dynamically analyzed.



```
rule process_inject
{
meta:
Classification = 32
Description = "Changed access protection of pages to RW/RWE and injected into"
Severity = 4

strings:
$ntget =/(Nt|Zw)GetProcessHeap:/
$ntquery =/(Nt|Zw)QuerySystemInformation(Process|Thread):/
$ntopen =/(Nt|Zw)OpenProcess:/
$ntalloc =/(Nt|Zw)AllocateVirtualMemory:/
$ntwrite =/(Nt|Zw)WriteVirtualMemory:[0-9A-F ]{6,12}\([0-6]{1}[0-9A-E]{2,4}./
$service =/(svchost|csrss|lsass|spoolsv|services|winlogon|explorer|iexplore|winsvc)\.exe/ nocase

condition:
all of them
and
(for any i in (1..#ntquery) : (@ntopen > @ntquery[i])) //sequence of query/open
and
(for any i in (1..#ntopen) : (@service > @ntopen[i])) //service name for NtOpenProcess
}
```

Figure 7-1 A sample Custom Behavioral Rules

After you import your Custom Behavioral Rules into Advanced Threat Defense, the malware detection and classification are based on these rules as well. Final severity result of sample analysis is determined as a maximum value from analysis methods mentioned above, including custom YARA rules.



Down Selector's Analysis:

Engine	GTI File Reputation	Gateway Anti-Malware	Anti-Malware	Custom Yara	Sandbox	Final
Threat Name	---	---	---	---	---	
Severity	None	None	None	4	2	4

This sample is malicious: final severity level 4

Figure 7-2 Final score influenced by custom YARA rule score

Considerations

- Advanced Threat Defense supports custom YARA rules only from Advanced Threat Defense release 3.2.0.
- Advanced Threat Defense 3.2.0 supports YARA version 1.0 only. So, all YARA features documented in YARA User's Manual for version 1.0 are supported.
- Advanced Threat Defense 3.4.8 supports YARA version 3.0.

- In an Advanced Threat Defense cluster setup, each node maintains its set of Custom Behavioral Rules separately. That is, the custom YARA rules that you define in the primary node are not sent to the secondary nodes automatically.
- There is no limit on the number of rules that you can include in your Custom Behavioral Rules file. Neither is there a limit on the size of this file. However, the number of rules and their complexity might affect the performance of Advanced Threat Defense.

Create the Custom Behavioral Rules file

Before you begin

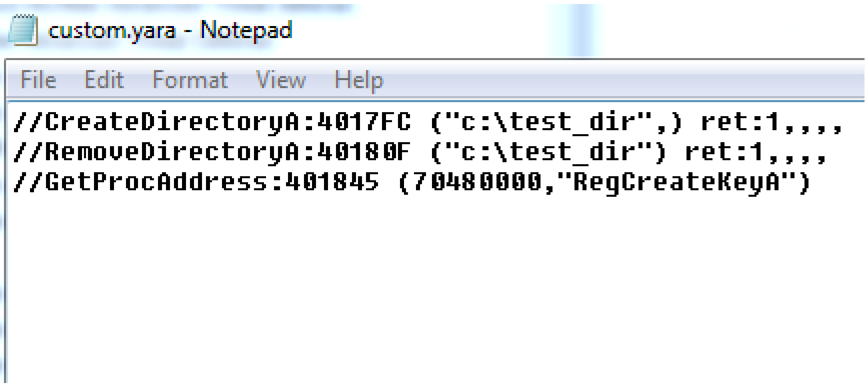
- You are familiar with all features of Custom Behavioral Rules that Advanced Threat Defense currently supports.
- You have identified the user API log of the sample that you want to use as a reference for creating your Custom Behavioral Rules.

Advanced Threat Defense applies the Custom Behavioral Rules on the User API log of an analyzed sample. To create Custom Behavioral Rules to catch a specific behavior, you can use the user API log of a sample that caused the same behavior. You can use YARA rules to catch runtime DLLs, file operations, registry operations, process operations, and other operations reported in analysis summary report for a sample. For example, to catch a specific runtime DLL, see a sample's user API log and write a YARA rule for that DLL.

Task

1 Create a text file and open it in a text editor such as Windows Notepad.

2 Enter the comments in the text file to track the APIs or data that are the sources for your Custom Behavioral Rules.



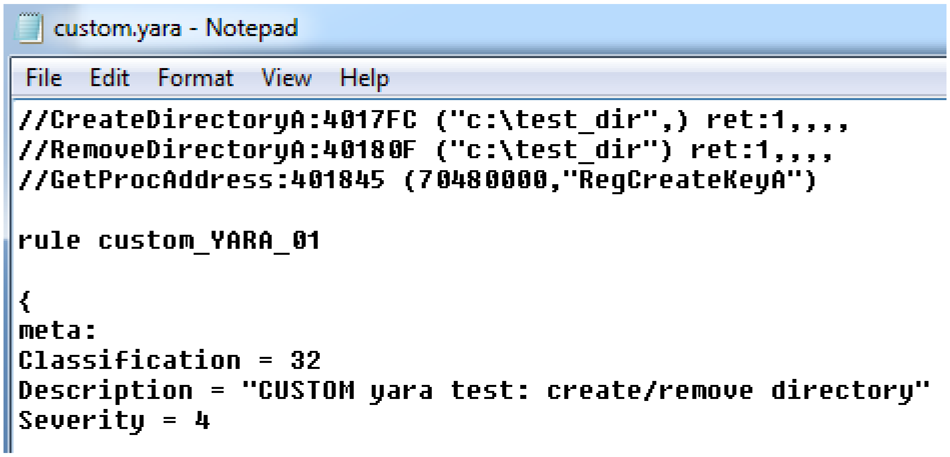
```
//CreateDirectoryA:4017FC ("c:\test_dir",) ret:1,,,,
//RemoveDirectoryA:40180F ("c:\test_dir") ret:1,,,,
//GetProcAddress:401845 (70480000,"RegCreateKeyA")
```

Figure 7-3 Comments for the custom YARA rules file

3 Write the first rule and provide it a name.

4 Enter the metadata for the rule.

Metadata is mandatory for standard rules and optional for helper rules. Regarding custom YARA rules, metadata can contain *classification*, *description*, and *severity*. Use a [metadata field name] = [string/value] format to define all these three metadata fields. These fields are case-insensitive.



```
//CreateDirectoryA:4017FC ("c:\test_dir",) ret:1,,,,
//RemoveDirectoryA:40180F ("c:\test_dir") ret:1,,,,
//GetProcAddress:401845 (70480000,"RegCreateKeyA")

rule custom_YARA_01

{
meta:
Classification = 32
Description = "CUSTOM yara test: create/remove directory"
Severity = 4
```

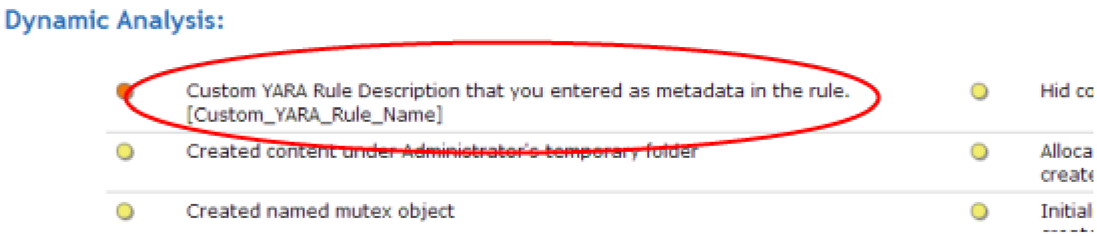
Figure 7-4 Metadata for a custom YARA rule

a Optionally, enter the classification value for Custom Behavioral Rules. Classification is the malware classification category to which a behavioral rule belongs. Use the following information to calculate the classification value.

Classification	Value
Persistence, Installation Boot Survival	1
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	2
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	4
Spreading	8
Exploiting, Shellcode	16
Networking	32
Data spying, Sniffing, Keylogging, Ebanking Fraud	64

For example, if a YARA rule describes a malware that attempted to do spreading (value 8), installation boot survival (value 1), and networking (value 32) then total classification result is 8+1+32 = 41.

b Enter the description for the rule, which is displayed in the analysis reports.



Dynamic Analysis:

Custom YARA Rule Description that you entered as metadata in the rule. [Custom_YARA_Rule_Name]

Hid co

Created content under Administrator's temporary folder

Alloca create

Created named mutex object

Initial

Figure 7-5 Custom Behavioral Rules name and description in the reports

c Enter a severity value for the behavior described by the YARA rule.

Severity value must be an integer from 1–5, with 5 indicating most malicious behavior. Severity values are irrelevant for helper rules.

5 From the **Analysis** | **Analysis Results** page, open the user API log report of the sample, which you plan to use as a reference to create the Custom Behavioral Rules.

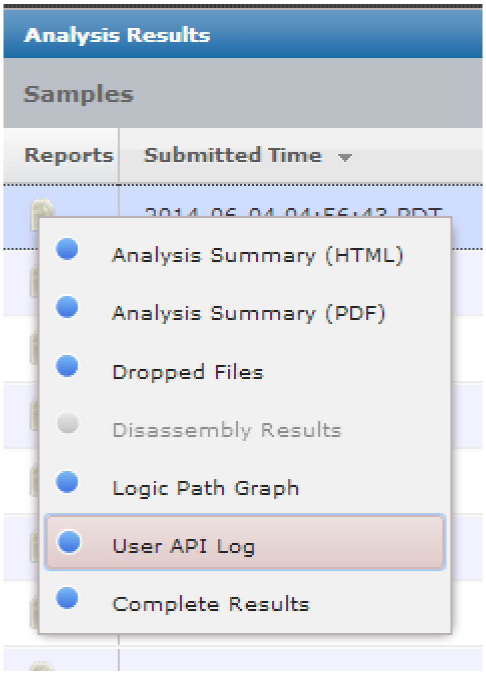
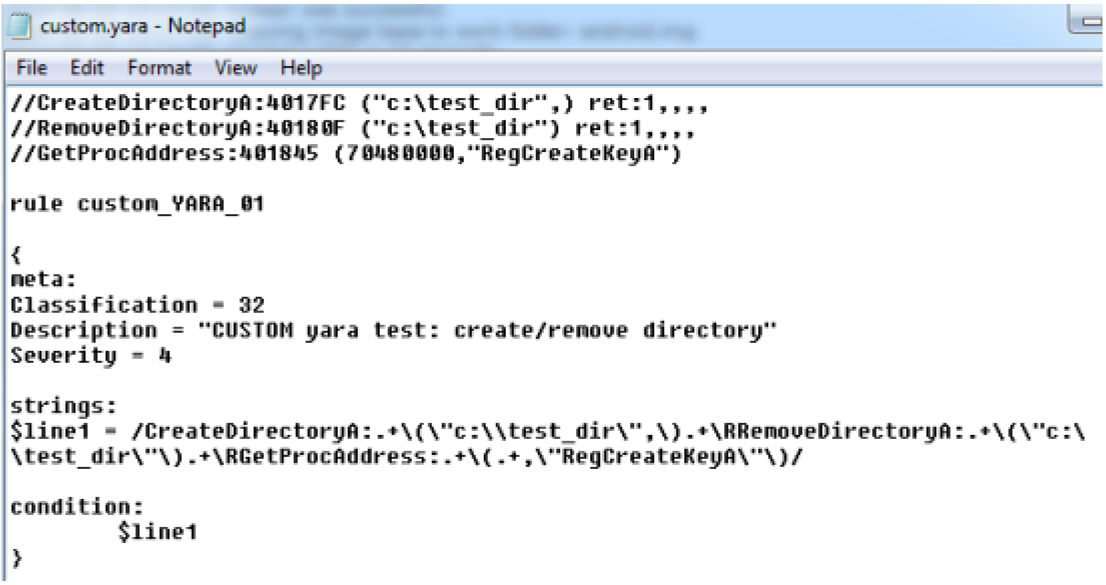


Figure 7-6 User API log as a reference for custom YARA rules

6 Enter the strings and conditions according to YARA syntax.



```
//CreateDirectoryA:4017FC ("c:\test_dir",) ret:1,,,,
//RemoveDirectoryA:40180F ("c:\test_dir") ret:1,,,,
//GetProcAddress:401845 (70480000,"RegCreateKeyA")

rule custom_YARA_01

{
meta:
Classification = 32
Description = "CUSTOM yara test: create/remove directory"
Severity = 4

strings:
$line1 = /CreateDirectoryA:.+\(\"c:\\test_dir\",\).+\RRemoveDirectoryA:.+\(\"c:\
\test_dir\"\).+\RGetProcAddress:.+\(.+,\"RegCreateKeyA\"\)/

condition:
        $line1
}
```

Figure 7-7 A custom YARA rule

7 Add more rules according to your requirement in the same custom YARA text file and save the file when complete.

Define Custom Yara Scanner

Custom Yara Scanner is also a set of YARA rules, similar to Custom Behavioral rules. The two differ in the fact that Custom Behavioral Rules is applied on the User API log of an analyzed sample, whereas, Custom Yara Scanner serves as an analyzing option in analyzer profile before analysis. Custom Yara Scanner is available as a static analysis option with no dependency on dynamic analysis.

Create Custom YARA Scanner files

YARA Scanner files is a set of rules written in accordance with YARA manual. These rules are user defined, written to identify any specific pattern in a file. If **Custom YARA Scanner** is enabled in your analyzer profile as an analyzing option, Advanced Threat Defense checks for a presence of these user defined rules in the samples being analyzed. If any defined rule is present in a file analyzed, then after the analysis **Very High** severity is displayed in the analysis report with threat name as the rule name. If defined rule is not present in the file analyzed, then **Unverified** is displayed in the analysis report for the file.

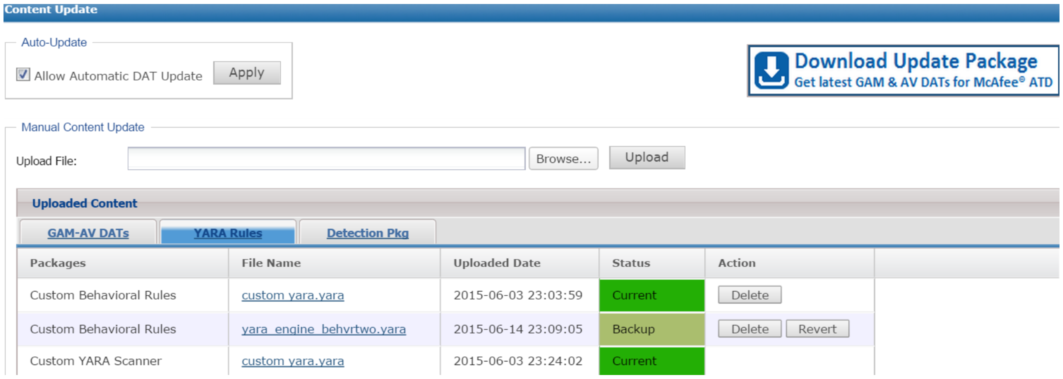
Import Custom Behavioral Rules and Custom Yara Scanner Rules

Before you begin

You have defined your Custom Behavioral Rules and Custom Yara Scanner Rules in a text file.

After you create your YARA rules in a text file, you import this file into Advanced Threat Defense using the Advanced Threat Defense web application.

> Advanced Threat Defense allows you to import a maximum of two versions of YARA rules at any given time. The version uploaded later becomes **Current** by default, rendering the previous one as **Backup**. Rules defined in DAT file designated as **Current** are applied for malware detection.



Content Update

Auto-Update

☑ Allow Automatic DAT Update

Manual Content Update

Upload File:

Uploaded Content

Packages	File Name	Uploaded Date	Status	Action
Custom Behavioral Rules	custom_yara.yara	2015-06-03 23:03:59	Current	Delete
Custom Behavioral Rules	yara_engine_behvrtwo.yara	2015-06-14 23:09:05	Backup	Delete Revert
Custom YARA Scanner	custom_yara.yara	2015-06-03 23:24:02	Current	

Task

1 Select **Manage** | **Image & Software** | **Content Update**.

2 In the **Uploaded Content** area, click on the **YARA Rules** tab.

3 Click **Browse** and locate the Custom Behavioral Rules or Custom Yara Scanner Rules you want to import.

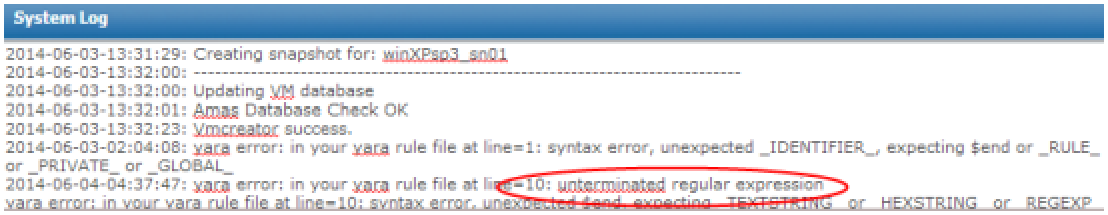
4 In the pop-up that appears subsequently, select the type of YARA file (Custom Behavioral Rules or Custom Yara Scanner Rules) to be imported.

5 Click **Upload** to import the file.

- If the Custom Behavioral Rules file is imported successfully, the **Custom YARA Scanner Rules uploaded successfully** message is displayed. If the Custom Behavioral Rules file is imported successfully, the **Custom YARA Scanner Rules uploaded successfully** message is displayed.

- If there are syntax errors in the Custom Behavioral Rules file, the **Uploaded file contains invalid Custom Behavioral Rules. Please check system log for more details.** message is displayed. If there are syntax errors in the Custom Behavioral Rules file, the **Failed to Execute YaraEngineUtility** message is displayed. You can review the system log for the details of the error.

Select **Manage** | **System Log** to open the system log, where the errors are detailed.



```
2014-06-03-13:31:29: Creating snapshot for: winXPsp3_sn01
2014-06-03-13:32:00: ------------------------------------------------------------------------
2014-06-03-13:32:00: Updating VM database
2014-06-03-13:32:01: Amas Database Check OK
2014-06-03-13:32:23: Vmcreator success.
2014-06-03-02:04:08: yara error: in your yara rule file at line=1: syntax error, unexpected _IDENTIFIER_, expecting $end or _RULE_
or _PRIVATE_ or _GLOBAL_
2014-06-04-04:37:47: yara error: in your yara rule file at line=10: unterminated regular expression
yara error: in your yara rule file at line=10: syntax error, unexpected $end, expecting _TEXTSTRING_ or _HEXSTRING_ or _REGEXP_
```

Figure 7-8 Details of the error

If you delete Current, the Backup file automatically assumes the role of Current. Click **Revert** to reinstate the Backup file as the Current file.

> In Load balancing scenario, the **Custom Yara Scanner** files need to be uploaded manually in primary node, secondary node, and Backup node using aforementioned instruction. The **Custom Yara Scanner** analyzing option is then enabled in the **Analyzer Profile** section of the primary node.

Modify Custom Behavioral Rules and Custom Yara Scanner file

Before you begin

You have imported the custom YARA text file into Advanced Threat Defense.

After you import the Custom Behavioral Rules and Custom Yara Scanner file, you might want to add some more rules or modify some of the existing rules. For example, you might want to change the severity value for a rule.

Task

1 Select **Manage** | **Image & Software** | **Content Update**.

2 In the **Uploaded Content** area, click on the **YARA Rules** tab.

3 Click the link under **File Name** to download the file from the Advanced Threat Defense database onto your client.

4 Open the file that you downloaded in a text editor and make the required changes. When complete, save the file.

You can rename this file according to your requirement.

5 Import the modified file into Advanced Threat Defense.

Enable or disable Custom Behavioral Rules

Before you begin

You have imported the Custom Behavioral rules text file into Advanced Threat Defense.

After you import the Custom Behavioral Rules, you can disable the them when not required. For example, you might want to disable them for reasons such as troubleshooting.

Task

1. Select **Manage** | **Custom Behavioral Rules.**

2. Deselect or select the **Enable Custom Behavioral Rules** checkbox.

   If you want to enable the Custom Behavioral rules that are currently present in the Advanced Threat Defense database, select **Enable Custom Behavioral Rules** and click **Submit.** That is, you need not import the Custom Behavioral rules text file again.

Update DAT version for McAfee Gateway Anti-Malware and Anti-Virus

Advanced Threat Defense allows you to import a maximum of two versions of DAT for Gateway Anti-Malware Engine and Anti-Virus at any given time. The DAT version uploaded later becomes **Current** by default, rendering the previous one as **Backup**. The DAT file designated as **Current** is used for malware detection.

Task

1. Select **Manage** | **Image & Software** | **Content Update**.

2. Click **Download Update Package** in the upper right corner of your screen or alternatively download the update package from the following link: https://contentsecurity.mcafee.com/update . Follow the subsequent instructions to download the latest versions of DAT available for Gateway Anti-Malware Engine and Anti-Virus.

3. Click **Browse** and locate the DAT files for Gateway Anti-Malware Engine and Anti-Virus you want to import.

4. Click **Upload** to import the file.

   If you delete the Current file, the Backup file automatically assumes the role of Current. Click **Revert** to reinstate the Backup file as the Current file.

   > In you want your DAT versions to be updated automatically, then select **Allow Automatic DAT Update** and click **Apply**. Your DAT file is updated with the latest version available. Also, any manual update done with **Allow Automatic DAT Update** enabled is overridden in the subsequent automatic DAT update cycle, automatically. Therefore, it is recommended to deselect **Allow Automatic DAT Update**, before making any manual update.

Update Detection Package

Advanced Threat Defense allows you to import a maximum of two versions of Detection Package at any given time. The version uploaded later becomes **Current** by default, rendering the previous one as **Backup**. The Detection Package designated as **Current** is applied for malware detection.

Task

1. Select **Manage** | **Image & Software** | **Content Update**.
2. Click the link provided to users for *system.msu* download. Contact support for any assistance on downloading the detection package.
3. Click **Browse** and locate the Detection Package you want to import.
4. Click **Upload** to import the file.

   If you delete the Current file, the Backup file automatically assumes the role of the Current. Click **Revert** to reinstate the Backup file as the Current file.

8 Analyzing malware

After you have configured Advanced Threat Defense, you can upload files and URLs for analysis. You can monitor the status of malware analysis using Advanced Threat Defense web application and then view the results.

Contents

Analyze files

Advanced Threat Defense analyzes the various files submitted to it via different channels. The analysis includes Static analysis and Dynamic analysis based on the configuration in the analyzer profile.

- The following are the methods you can follow to submit files:
  - Manually upload the file using the Advanced Threat Defense web application.
  - Post the file on the FTP server hosted on the Advanced Threat Defense Appliance.
  - Use the RESTful APIs of the Advanced Threat Defense web application to upload the file. See the *McAfee Advanced Threat Defense APIs Reference Guide.*
  - Integrate Advanced Threat Defense with Network Security Platform and McAfee Web Gateway. Then, these applications automatically submit samples to Advanced Threat Defense. See the corresponding documentation.
- The maximum file size supported is 128 MB if you use the Advanced Threat Defense web application, its restful APIs, or McAfee Web Gateway.
- Unicode is supported for the file name of samples. A file name can be up to 200 bytes long. A file names can contain non-English characters and special characters.

> File names are displayed as the MD5 hash value of the file if the following characters are used: "'`<>|;*?#$*
>
> For example, if the file name of a submitted sample is vtest;32.exe, then Advanced Threat Defense displays the file name as e2cfe1c89703352c42763e4b458fc356.exe.

- Static analysis of Visual Basic for Applications scripts (VBA scripts) embedded inside a Microsoft Office application takes place inside the VMs. This analysis enhances the chance of identifying any threat disguised as a VBA script.

- Pre-filtering of files and applications pertaining to Microsoft Office 2003 and earlier and Microsoft Office 2007 and later is catered to. The pre-filtering functionality ascertains the high confidence Microsoft Office samples as clean, even before these samples are submitted for dynamic analysis. This reduces load on the VMs.
- Dynamic analysis of Flash files takes place after installing a browser-based Flash plug-in on VMs.

Table 8-1 Supported file types

File Types	Static Analysis	Dynamic Analysis
32-bit Portable Executables (PE) files; 64-bit PE+ files	.exe, .dll, .scr, .ocx, .sys, .com, .cpl	.exe, .dll, .scr, .ocx, .sys, .com, .cpl
Microsoft Office Suite documents	.doc, .docx, .xls, .xlsx .ppt, .pptx, .rtf	.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf
Adobe	PDF files, Adobe Flash files (SWF)	PDF files, Adobe Flash files (SWF)
Compressed files	.cab, .7z, .zip, .rar , msi	.zip, .cab, .7z, .msi
Android application package	.apk	.apk
Java	Java Archives (JAR), CLASS, Java Script, Java bin files	Java Archives (JAR), CLASS, Java Script, Java bin files
Image files	.jpeg, .png, .gif	Not supported
Other file types	.cmd, .bat, .vbs, .xml, .url, .htm	.cmd, .bat, .vbs, .xml, .url, .htm

Upload files for analysis using Advanced Threat Defense web application

Before you begin

Make sure that the required analyzer profile is available.

When you use the Advanced Threat Defense web application to submit a file for analysis, you must select an analyzer profile. This analyzer profile overrides the default analyzer profile associated with your user account.

Task

1. Select **Analysis** | **Manual Upload.**
2. On the **Manual Upload** page, specify the details as per your requirement.

Table 8-2 Option definitions

Option	Definition
File	Either drag and drop the malware file from Windows Explorer or click **Browse** and select the file. If you want to submit multiple files, upload them in a .zip file. • If you are uploading a password-protected .zip file, make sure you have provided the password in the analyzer profile that you want to use for analysis. • If dynamic analysis is required, the files in the .zip file are executed on different instances of the analyzer VM. If enough analyzer VMs are not available, some of the files are in the pipeline until analyzer VMs are available. • Because the files in the .zip file are analyzed separately, separate reports are created for each file. • Unicode is supported for the file name of samples. A file names can contain non-English characters and special characters. File names are displayed as the MD5 hash value of the file if the following characters are used: "'`<>|;*?#$* • The file name can be up to 200 bytes in length.
Analyzer Profile	Select the required analyzer profile for the sample.
Advanced	Click to specify additional parameters for analyzing the sample. The **Advanced** options are available only when you manually submit the file using Advanced Threat Defense web application. • **User Interactive Mode:** Upon execution, some malware requires user input. This is typically done to check if the malware is being analyzed in a sandbox. In the absence of user input, the malware might take an alternative execution path or suspend further execution. If you select this option, you can access the actual analyzer VM on which the malware is executed and provide the required input. • **Skip files if previously analyzed:** Use this function to avoid reanalyzing samples. After you make the required selections, click **OK**.
Submit	Click to upload the file to Advanced Threat Defense for analysis.

Tasks

- *Upload URLs for analysis in user-interactive mode* on page 285
- *Upload samples for analysis in skip analysis mode* on page 287

Upload URLs for analysis in user-interactive mode

Before you begin

Make sure that the required analyzer profile is available with sandbox and malware Internet access options selected.

To completely execute some malware, user intervention might be required.

For example, a default setting in the analyzer VM might pause the execution unless the setting is manually overridden. Some files might display dialog boxes, where you are required to make a selection or a confirmation. Malware demonstrates such behavior to determine if they are being executed in a sandbox. The behavior of the malware might vary based on your intervention. When you submit files in user-interactive mode, the analyzer VM opens in a pop-up window on your client computer and you can provide your input when prompted.

You can upload files to be executed in the user-interactive mode. This option is available only when you manually upload a file using the Advanced Threat Defense web application. For files submitted by other methods, such as FTP upload and files submitted by Network Security Platform, requests for user intervention by the malware are not honored. However, the screen shots of all such requirements are available in the **Screenshots** section of the **Analysis Summary** report. Then you can manually resubmit such files in the user-interactive mode to know the actual behavior of the file.

> For XMode, Google Chrome version 44.0.2403 and later, and Mozilla Firefox version 40.0.3 and later are supported. Microsoft Internet Explorer is not supported.

> Because the analyzer VM is opened in a pop-up window, make sure the pop-up blocker is disabled in your browser.

Task

1 Select **Analysis** | **Manual Upload.**

2 In the **File** field, click **Browse** and select the file you want to submit for analysis, or drag and drop the file into the specified box.

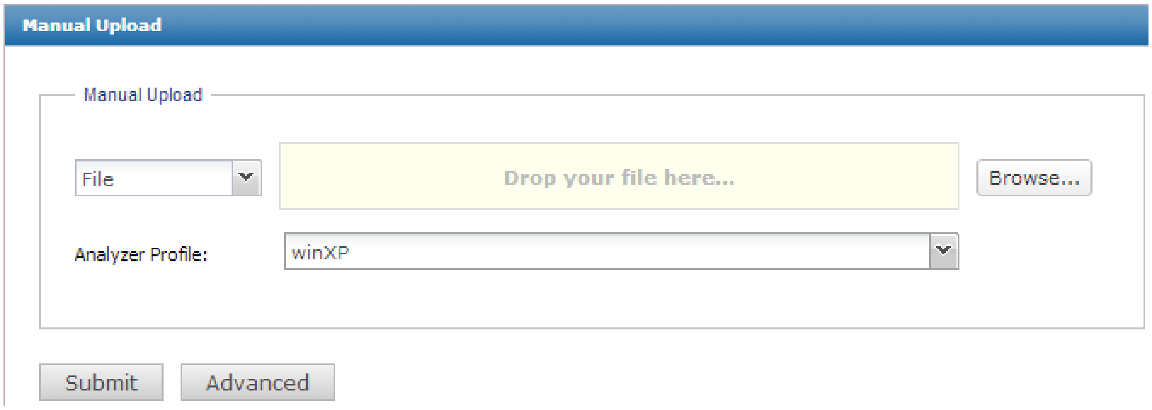
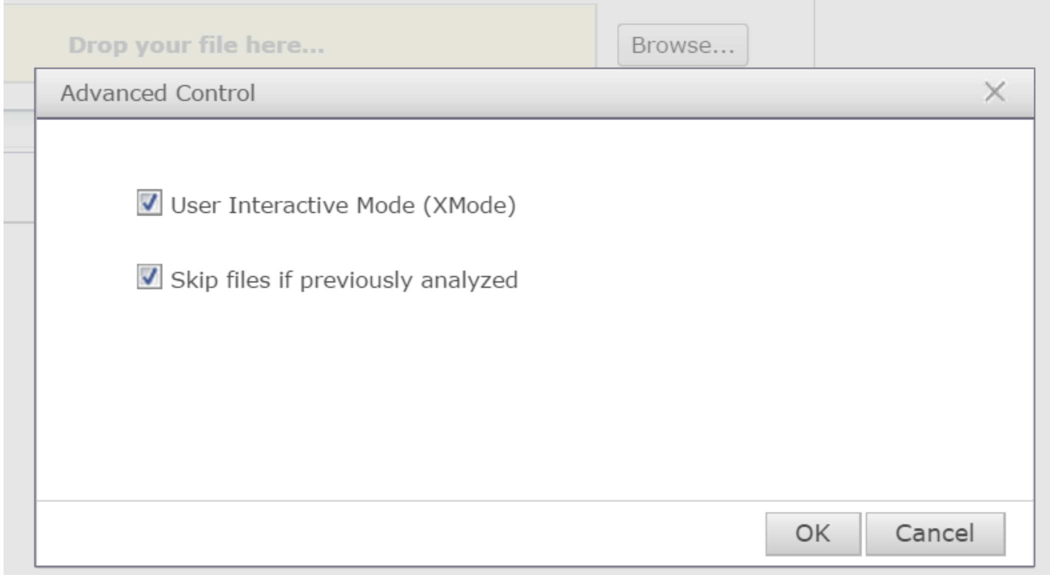


Figure 8-1 Submit the file

3 In the **Analyzer Profile** field, select the required analyzer profile from the drop-down list.

4 Click **Advanced** and select **User Interactive Mode (XMode).**



☑ User Interactive Mode (XMode)

☑ Skip files if previously analyzed

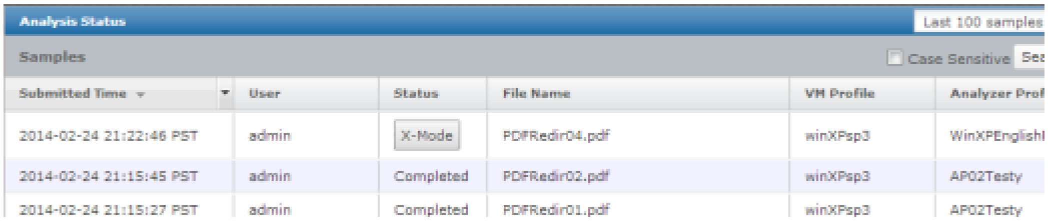
Figure 8-2 Select User Interactive Mode (XMode)

5 Click **OK**, then click **Submit.**

The sample is uploaded to Advanced Threat Defense and a success message with the details are displayed.

6 Click **OK** in the **Uploaded File Successfully** dialog box.

7 Click **OK** to go to the **Analysis Status** page.



Submitted Time	User	Status	File Name	VM Profile	Analyzer Prof
2014-02-24 21:22:46 PST	admin	X-Mode	PDFRedir04.pdf	winXPsp3	WinXPEnglishI
2014-02-24 21:15:45 PST	admin	Completed	PDFRedir02.pdf	winXPsp3	AP02Testy
2014-02-24 21:15:27 PST	admin	Completed	PDFRedir01.pdf	winXPsp3	AP02Testy

Figure 8-3 X-Mode in the Analysis Status page

8 On the **Analysis Status** page, click **X-Mode** for the corresponding record.

9 After the file execution completes, the VM automatically shuts down.

> Once the analysis is complete, you cannot use **Connect** to view the VNC session. If you click Connect, *a Failed to connect server* error message is displayed.

> When you click **Disconnect** , it only closes the VNC session from the client and displays a *VNC disconnected* error message. If you click **Connect**, it will connect back to the VNC session.

Upload samples for analysis in skip analysis mode

You can configure Advanced Threat Defense to skip analysis of the submitted samples, if the same has been analyzed previously.

Task

1 Select **Analysis** | **Manual Upload.**

2 In the **Manual upload** field, click **Browse** and select the file you want to submit for analysis or drag and drop the file into the specified box.

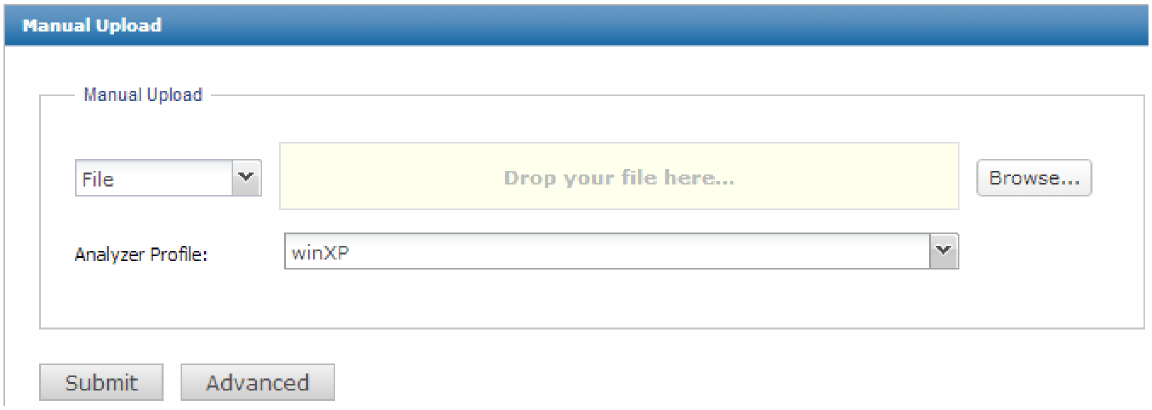


Figure 8-4 Submit the file

3 In the **Analyzer Profile** field, select the required analyzer profile from the drop-down list.

4 Click **Advanced** and select **Skip files if previously analyzed.**

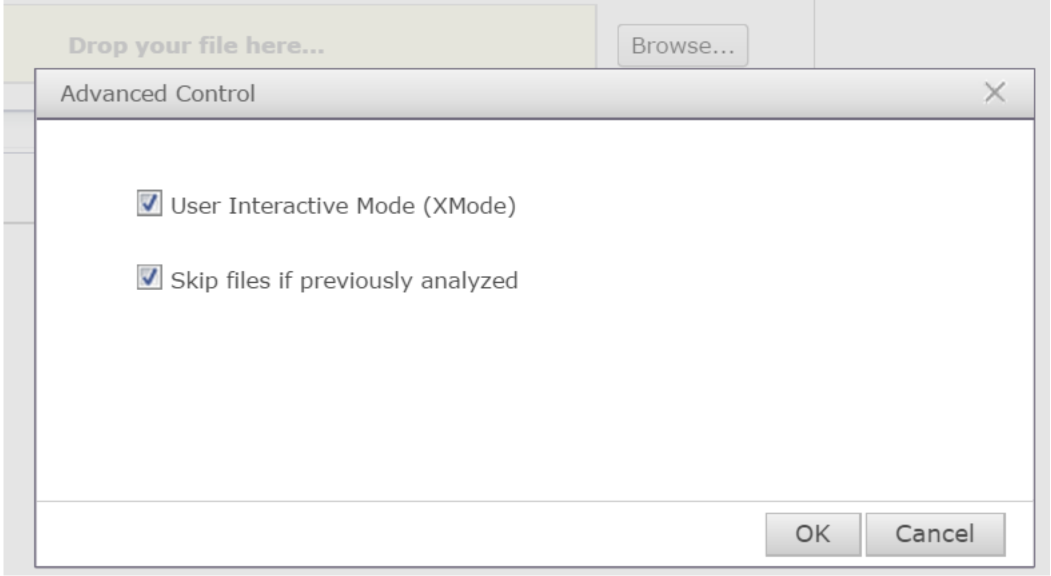

Drop your file here...
Browse...
Advanced Control
☑ User Interactive Mode (XMode)
☑ Skip files if previously analyzed
OK
Cancel

Figure 8-5 Skip files if previously analyzed

5 Click **OK**, then click **Submit.**

The sample is uploaded to McAfee Advanced Threat Defense and a success message with the details specifying that the submitted file was previously analyzed is displayed.

6 Click **OK** in the **Uploaded File Successfully** dialog box.

> Sample analysis is not skipped in the following scenarios:
> - If Analyzer Profile is modified after the last analysis
> - If the submitted sample was analyzed more than three days ago
> - If the samples are submitted via **URL Download** method

> If a previously analyzed .zip file is submitted again, a single sample from the .zip with highest severity is displayed.

Upload files for analysis using SFTP

Before you begin

- Your user name has **FTP Access** privilege. This is required to access the FTP server hosted on Advanced Threat Defense.
- You have created the required analyzer profile that you want to use.
- You have installed an FTP client on your machine.

Using SFTP, you can upload the supported file types to the FTP server on Advanced Threat Defense.

> By default, FTP is not a supported protocol for uploading samples. To use FTP to upload files, you must enable it using the `set ftp` CLI command. See set ftp on page 363.

Task

1. Open your FTP client and connect to Advanced Threat Defense using the following information.
   - Host — Enter the IP address of Advanced Threat Defense.
   - User name — Enter your Advanced Threat Defense user name.
   - Password — Enter your Advanced Threat Defense password.
   - Port — Enter 22, which is the standard port for SFTP. For FTP, enter 21.
2. Upload the files from the local site to the remote site, which is on Advanced Threat Defense.
3. In the Advanced Threat Defense web application, select **Analysis** | **Analysis Status** to monitor the status of the uploaded files.

Analyze URLs

Similar to how you submit a file for analysis, you can submit URL to Advanced Threat Defense for analysis in this release. Advanced Threat Defense analyzes the URL in an analyzer VM determined by the user profile, and reports the file analysis results. Advanced Threat Defense uses only the local blacklist and dynamic analysis for the downloaded file. In addition, the McAfee GTI reputation of the URL is reported. The behavior of the browser when opening the URL is also analyzed for malicious activity.

Follow these methods to submit URLs:

- Manually upload the URL using the Advanced Threat Defense web application.
- Use the restful APIs of Advanced Threat Defense web application to upload URLs. See the *Advanced Threat DefenseRESTful APIs Reference Guide.*

Malicious websites typically contain multiple types of malware. When a victim visits the website, the malware that suits the vulnerabilities present in the endpoint is downloaded. You can create multiple analyzer VMs, each with different operating systems, browsers, applications, browser plug-ins that are relevant to your network. Also, if the browsers and operating systems are unpatched, it might enable you to analyze the actual behavior of web sites.

The advantage of using Advanced Threat Defense is that, you can get a detailed report of previously unknown malicious domains, websites, and IP addresses as well as the current behavior of known ones. You can also get a detailed analysis report for even benign sites that are recently compromised.

Advanced Threat Defense does not analyze URLs contained within files submitted for analysis. For example, when a Network Security Sensor submits a Microsoft Word file, Advanced Threat Defense analyses the file for malware but does not analyze any URLs in the file.

How Advanced Threat Defense analyzes URLs?

To analyze URLs, select an analyzer profile that has both sandbox and Internet access enabled. Following is the process flow when you submit a URL for analysis to Advanced Threat Defense:

1. Advanced Threat Defense uses a proprietary procedure to calculate the MD5 hash value of the URL. Then, it checks this MD5 against its local blacklist.

   ℹ The local whitelist is not applicable for URLs.

2. It is assumed that the file that the URL refers to is of a supported file type. Then Advanced Threat Defense dynamically analyzes the file using the corresponding analyzer VM. It is assumed that the MD5 of the URL is not present in the blacklist or **Run All Selected** option is selected in the corresponding analyzer profile.

   ℹ GTI File Reputation, Anti-Malware, and Gateway Anti-Malware analyze options are not relevant for URLs.

3. Dynamic analysis and reporting for URLs is similar to that of files. It records all activities in the analyzer VM including registry operations, process operations, file operations, runtime DLLs, and network operations. If the webpage downloads any dropper files, Advanced Threat Defense dynamically analyzes these files as well and includes the results in the same report under embedded/dropped content section.

4. If a dropped file connects to other URLs, all these URLs are checked with TrustedSource for URL reputation and categorization.

ℹ Only HTTP, HTTPS, and FTP protocols are supported for URL analysis.

Upload URLs for analysis using Advanced Threat Defense web application

Before you begin

Make sure that the required analyzer profile is available with sandbox and malware Internet access options selected.

You can upload the URLs using two different options based on their requirements, using Advanced Threat Defense web application.

These options are available for manually uploading URLs:

- **URL**—The selected URL is sent to the analyzer VM, and the file pointed to by the URL is downloaded to the analyzer VM for analysis. For example, when a user submits the URL http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe, the URL is sent to the analyzer VM, then the putty.exe file is downloaded to the analyzer VM.
- **URL Download**—The selected URL is downloaded to the Advanced Threat Defense. The file which the URL is pointing to is downloaded locally in the Advanced Threat Defense and the downloaded file is then sent to the static analyzers and the analyzer VM for analysis. For example, when a user submits the URL http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe, the putty.exe file is downloaded to the Advanced Threat Defense, then sent to the analyzer VM.

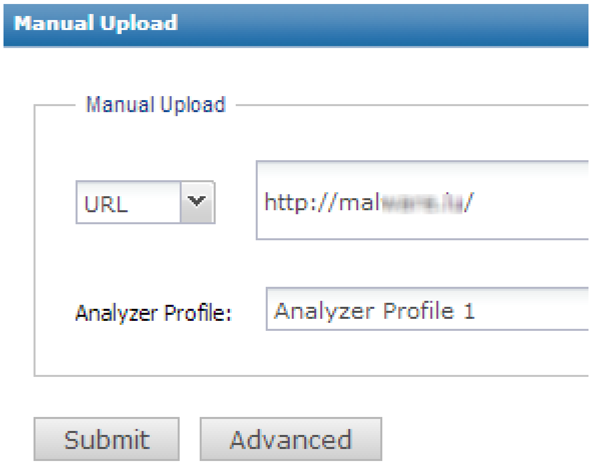
When you use the Advanced Threat Defense web application to submit a URL for analysis, select an analyzer profile. This analyzer profile overrides the default analyzer profile associated with your user account.

Manual upload using URL option

Task

1 Select **Analysis** | **Manual Upload.**

2 In the **Manual Upload** page, specify the details according to your requirement.



Manual Upload

Manual Upload

URL: http://mal[redacted]/

Analyzer Profile: Analyzer Profile 1

Figure 8-6 Submit a URL for malware analysis

Table 8-3 Option definitions

Option	Definition
URL Upload method	Select an upload method from the drop-down list: • **URL**—The URL is analyzed directly on the VM analyzer. • **URL Download**—The file referred to by the URL is downloaded to the Advanced Threat Defense appliance, and the downloaded file is sent to the VM analyzer for analysis. Only HTTP, HTTPS, and FTP are supported. So, specify the protocol identifier in the URL. Preferably enter the entire URL. When Advanced Threat Defense dynamically analyzes the URL, the browser might add any missing items. For example, if you enter `http://google.com`, the browser in the analyzer VM might correct it to `http://www.google.com`
Analyzer Profile	Select the required analyzer profile for the sample. Only those analyzer profiles that have sandbox and malware Internet access are listed.
Advanced	Click to specify user interactive mode for analyzing the URL. The **Advanced** option is available only when you manually submit the file using Advanced Threat Defense web application. Upon execution, some malware require user input. This is typically done to check if the malware is being analyzed in a sandbox. In the absence of user input, the malware might take an alternative execution path or even might suspend further execution. If you select this option, you can access the actual analyzer VM on which the malware is executed and provide the required input. This is similar to executing files in user-interactive mode. See Upload URLs for analysis in user-interactive mode on page 285.
Submit	Click to upload the URL to Advanced Threat Defense for analysis. A message box is displayed after the URL is uploaded successfully. • File Name — The URL that you submitted • File Size — Size of the sample • MD5 — The MD5 hash value as computed by Advanced Threat Defense • Mime Type

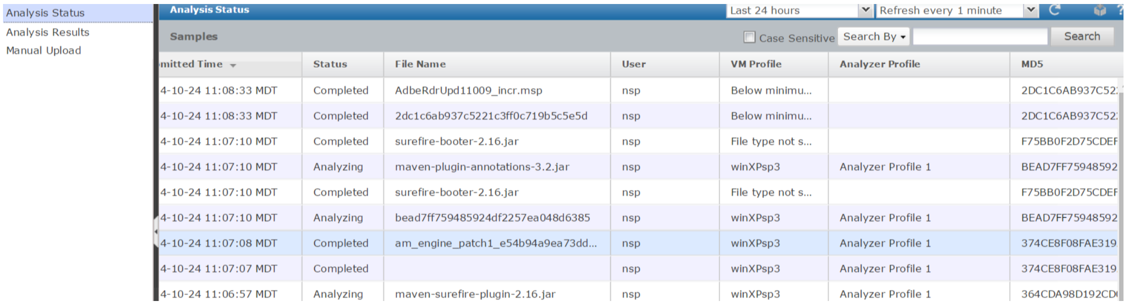
3 Click **Submit**.

Configure the Analysis Status page

Task

1 Select **Analysis** | **Analysis Status.**

The **Analysis Status** page lists the status for the submitted files.



Last 24 hours
Refresh every 1 minute

mitted Time	Status	File Name	User	VM Profile	Analyzer Profile	MD5
4-10-24 11:08:33 MDT	Completed	AdbeRdrUpd11009_incr.msp	nsp	Below minimu...		2DC1C6AB937C52
4-10-24 11:08:33 MDT	Completed	2dc1c6ab937c5221c3ff0c719b5c5e5d	nsp	Below minimu...		2DC1C6AB937C52
4-10-24 11:07:10 MDT	Completed	surefire-booter-2.16.jar	nsp	File type not s...		F75BB0F2D75CDEF
4-10-24 11:07:10 MDT	Analyzing	maven-plugin-annotations-3.2.jar	nsp	winXPsp3	Analyzer Profile 1	BEAD7FF75948592
4-10-24 11:07:10 MDT	Completed	surefire-booter-2.16.jar	nsp	File type not s...		F75BB0F2D75CDEF
4-10-24 11:07:10 MDT	Analyzing	bead7ff759485924df2257ea048d6385	nsp	winXPsp3	Analyzer Profile 1	BEAD7FF75948592
4-10-24 11:07:08 MDT	Completed	am_engine_patch1_e54b94a9ea73dd...	nsp	winXPsp3	Analyzer Profile 1	374CE8F08FAE319
4-10-24 11:07:07 MDT	Completed		nsp	winXPsp3	Analyzer Profile 1	374CE8F08FAE319
4-10-24 11:06:57 MDT	Analyzing	maven-surefire-plugin-2.16.jar	nsp	winXPsp3	Analyzer Profile 1	364CDA98D192CD

Figure 8-7 Status of files submitted for analysis

> If you do not have administrative permissions, only those files that you submitted are listed. A user with administrative permissions can view the samples provided by any user.

2 From the drop-down lists, select the criteria for viewing and refreshing the status of files being analyzed.

- Set the criteria to display records on the **Analysis Status** page.

  The default refresh interval is 1 minute.

- Set the frequency at which the **Analysis Status** page is refreshed.

  By default, results from the last 24 hours are displayed. You can specify this criteria based on time or number. For example, you can select to view the status for files submitted in the last 5 minutes or for the last 100 samples.

  > To refresh the Analysis Status page now, click ↻

3 Filter the displayed records to locate the required ones.

Table 8-4 Filtering options

Option	Definition
Search	Specify the parameter that you want to use to filter the records. Click **Search** and select one or more of the following parameters: • Set the criteria to display records on the **Analysis Status** page. • **File Name:** Select if you want to filter based on the starting characters of the file name. For example, if you select this option and enter *cal* as the search string then the status for files names that start with *cal* are listed. • **MD5:** Select if you want to filter based on the starting characters of the MD5 hash value. • **VM Profile:** Select if you want to filter based on the VM profiles available. • **File Type:** The type of file format that is submitted for analysis. • **Analyzer Profile:** The analyzer profile that was referred to for the analysis. If the file was analyzed only by a static method, that is displayed. • **User:** The log on name of the user who submitted the file for analysis. • **Source IP:** The IP of the host that sent the analyzed file. This is relevant only for files automatically submitted by other McAfee products such as Network Security Platform. • **Destination IP:** The IP of the targeted host. Similar to the source IP, this is not relevant for manually submitted files. • **Job ID:** This is a unique number assigned to all the files. • **Task ID:** This is a unique number assigned to all the files. The **Task ID** and **Job ID** are different for compressed files, and are same for uncompressed files. • **URL:** List of URL that is submitted for analysis. Enter the search string in the adjacent text box.
Case Sensitive	Select if you want to make the search case sensitive.

Suppose that you have selected **File Name** and **Status** as the criteria, selected **Case Sensitive**, and specified *Com*. All the records in the completed state and file names starting with the characters *Com* are listed.

Table 8-5 Column definitions

Column	Definition
Submitted Time	The time stamp when the file was submitted for analysis.
Status	The current status of analysis. • **Waiting —** Typically, this indicates that Advanced Threat Defense is waiting for an analyzer VM to dynamically analyze the file. • **Analyzing —** Indicates that the analysis is still in progress. • **Completed —** Indicates that the analysis is complete for the file. Double-click the record to see the complete report. • **Discarded —** Indicates that the analysis of files is aborted after the reboot. Analyzer VM dynamically re-analyzes the files.
File Name	The name of the file that you submitted for analysis.

Table 8-5 Column definitions *(continued)*

Column	Definition
VM Profile	The VM profile used for dynamic analysis. If the file was analyzed only by a static method, that is displayed.
MD5	The MD5 hash value of the file as calculated by Advanced Threat Defense.
Analyzer Profile	The analyzer profile that was referred to for the analysis. If the file was analyzed only by a static method, that is displayed.
User	The log on name of the user who submitted the file for analysis.
Source IP	The IP of the host that sent the analyzed file. This is relevant only for files automatically submitted by other McAfee products such as Network Security Platform.
Destination IP	The IP of the targeted host. Similar to the source IP, this is not relevant for manually submitted files.

4 Hide the columns that you do not require.

   a Move the mouse over the right corner of a column heading and click the drop-down arrow.

   b Select **Columns.**

   c Select only the required column names from the list.

   > You can click a column heading and drag it to the required position.

5 To sort the records based on a particular column name, click the column heading.

   You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**. By default, the records are sorted in descending oreder based on the **Submitted Time** column.

6 To save the Analysis Status page settings, click 💾

View the analysis results

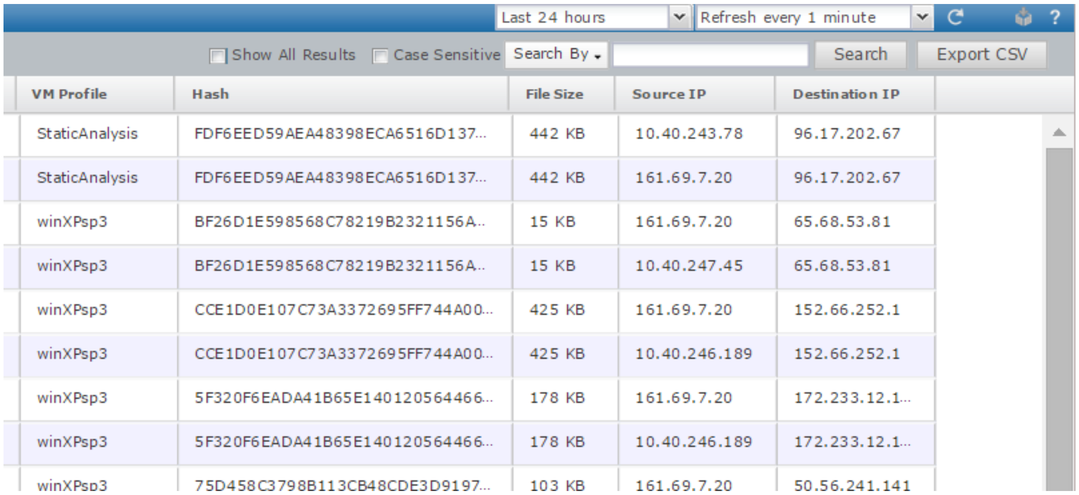
After you submit a file for analysis, you can view the results in the **Analysis Results** page.

> Older reports are deleted when the data disk of Advanced Threat Defense is 75 percent full. You can view the current data disk space available in the **System Health** monitor of the **Dashboard**. If you configure the options under **FTP Result Output** in the **User Management** page, then Advanced Threat Defense saves the results locally as well as sends them to the configured FTP server for your long-term use.

Task

1 Select **Analysis** | **Analysis Results.**

The **Analysis Results** page lists the status for the completed files.



VM Profile	Hash	File Size	Source IP	Destination IP
StaticAnalysis	FDF6EED59AEA48398ECA6516D137...	442 KB	10.40.243.78	96.17.202.67
StaticAnalysis	FDF6EED59AEA48398ECA6516D137...	442 KB	161.69.7.20	96.17.202.67
winXPsp3	BF26D1E598568C78219B2321156A...	15 KB	161.69.7.20	65.68.53.81
winXPsp3	BF26D1E598568C78219B2321156A...	15 KB	10.40.247.45	65.68.53.81
winXPsp3	CCE1D0E107C73A3372695FF744A00...	425 KB	161.69.7.20	152.66.252.1
winXPsp3	CCE1D0E107C73A3372695FF744A00...	425 KB	10.40.246.189	152.66.252.1
winXPsp3	5F320F6EADA41B65E140120564466...	178 KB	161.69.7.20	172.233.12.1...
winXPsp3	5F320F6EADA41B65E140120564466...	178 KB	10.40.246.189	172.233.12.1...
winXPsp3	75D458C3798B113CB48CDE3D9197...	103 KB	161.69.7.20	50.56.241.141

Figure 8-8 Status of files submitted for analysis

> If you do not have admin permissions, only those files that you submitted are listed. A user with admin permissions can view the samples submitted by all users.

> Click on **Export CSV** to export locally the status of completed files in CSV format.

2 Specify the criteria for viewing and refreshing the records in the **Analysis Results** page.

a Set the criteria to display records in the **Analysis Results** page.

By default, the results for the files completed in the last 24 hours are shown.

You can specify this criteria based on time or number. For example, you can select to view the files for which the analysis was completed in the last 5 minutes or for the last 100 completed files.

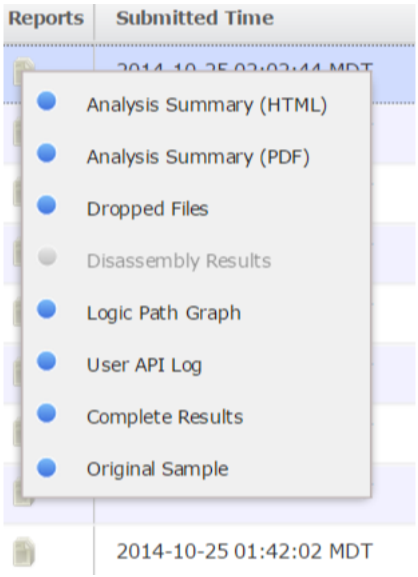
b Set the frequency at which the **Analysis Results** page must refresh itself.

The default refresh interval is 1 minute.

c To refresh the **Analysis Results** page now, click ↻.

Table 8-6 Column definitions

<table>
<tr><th>Column</th><th>Definition</th></tr>
<tr><td><b>Reports</b></td><td>
Click 📄 to display the types of reports available for the sample.



Click any of the enabled reports to view the corresponding details. A specific report is enabled only if it is relevant to the analyzed file and also selected in the corresponding analyzer profile.

- **Analysis Summary (HTML)** — This is the comprehensive report that is available for all file types. This report is also displayed when you double-click a record.
- **Analysis Summary (PDF)** — Select this to view the report in PDF.
- **Dropped Files** — Select this report to view the files that the analyzed sample created during dynamic analysis.
- **Disassembly Results** — Select this to view the assembly language code reverse-engineered from the file. This report is relevant only for sample types such as .exe and .dll.
- **Logic Path Graph** — Select this to view a graphical representation of which subroutines were executed during the dynamic analysis and which were not.
- **Dynamic Execution Logs** — Select this to view the Windows user-level DLL API calls made directly by the sample during dynamic analysis.
- **Complete Results** — Click to download the .zip file containing all the report types to your local machine.
- **Original Sample** — Click to download the originally submitted sample.
</td></tr>
<tr><td><b>Submitted Time</b></td><td>The time stamp when the file was submitted for analysis.</td></tr>
<tr><td><b>Severity</b></td><td>The severity of the submitted file.</td></tr>
<tr><td><b>File Name</b></td><td>The name of the file that you submitted for analysis.</td></tr>
<tr><td><b>User</b></td><td>The log on name of the user who submitted the file for analysis.</td></tr>
<tr><td><b>Analyzer Profile</b></td><td>The analyzer profile that was referred to for the analysis.</td></tr>
</table>

Table 8-6 Column definitions *(continued)*

Column	Definition
VM Profile	The VM profile used for the dynamic analysis. If only static was used, that is displayed.
Hash	The MD5 hash value of the file as calculated by Advanced Threat Defense.
File Size	The size of the analyzed file in KB.
Source IP	The IP of the host that sent the analyzed file. This is relevant only for files automatically submitted by other McAfee products such as Network Security Platform.
Destination IP	The IP of the targeted host. Similar to the source IP, this is not relevant for manually submitted files.

3 Choose to hide the columns that you do not require.

a Move the mouse over the right corner of a column heading and click the drop-down arrow.

b Select **Columns**.

c Select only the required column names from the list.

> You can click a column heading and drag it to the required position.

4 To sort the records based on a particular column name, click the column heading.

You can sort the records in the ascending or descending order. Alternatively, move the mouse over the right corner of a column heading and click the drop-down arrow. Then select **Sort Ascending** or **Sort Descending**.

By default, very high severity files are shown at the top of the list.

5 To save the Analysis Results page settings, click

View the Threat Analysis report

The Threat Analysis report is an executive brief detailing key behaviors of the sample file. This report is available in HTML, text, PDF, XML, JSON, Open Indicators of Compromise (OpenIOC), and Structured Threat Information eXpression (STIX) formats.

The HTML, text, and PDF formats are mainly for you to review the analysis report. You can access the HTML and PDF formats from the Advanced Threat Defense web application. The HTML and text formats are also available in the reports .zip file for the sample, which you can download to your client computer.

The XML and JSON formats provide well-known malware behavior tags for high-level programming script to extract key information. Network Security Platform and McAfee Web Gateway use the JSON formats to display the report details in their user interfaces.

If the severity level of the sample is 3 and above, then the Threat Analysis report is available in OpenIOC (.ioc) and STIX (.stix.xml) formats. OpenIOC and STIX formats are universally recognized formats for sharing threat information. These formats enable you to effectively share the Analysis Summary reports with other security applications for a better understanding, detection, and containment of malware. For example, you can manually submit the OpenIOC and STIX reports to an application, which can query hosts for the indicators in the report. This way you can detect the infected hosts, and then take the required remedial actions to contain and remove the malware.

For generic information on OpenIOC, see http://www.openioc.org/. Regarding STIX, you can see https://stix.mitre.org/. The Threat Analysis report in the OpenIOC and STIX formats are available in the Complete Results zip file for the sample.

Task

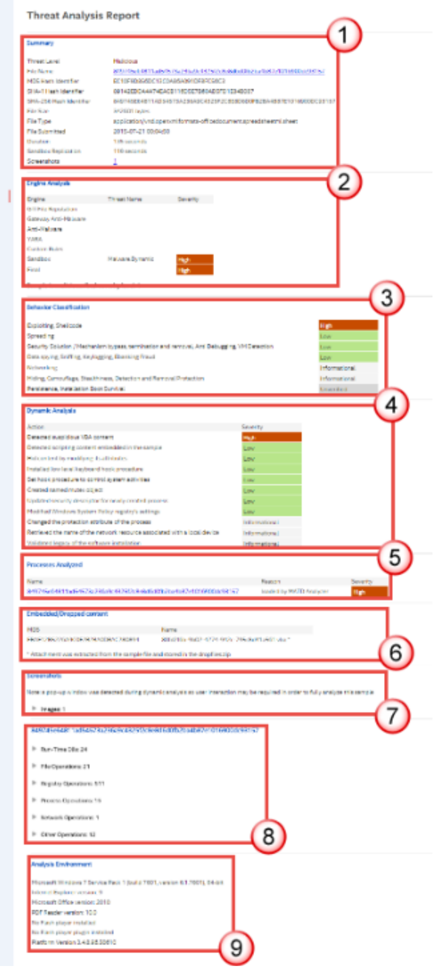
1. To access the Threat Analysis report in the Advanced Threat Defense web application, do the following:
   - a Select **Analysis | Analysis Results**.
   - b To view the HTML format of the report, click 📄 and then select **Analysis Summary (HTML)**.

     Alternatively, you can double-click the required record.
   - c To view the PDF of the report, click 📄 and then select **Analysis Summary (PDF)**.
2. To access the Threat Analysis report from the reports .zip file, do the following:
   - a Select **Analysis | Analysis Results**.
   - b Click 📄 and select **Complete Results**.
   - c Save the zipped reports on your local machine.

     The .zip file is named after the name of the sample file.
   - d Extract the contents of the .zip file.

     The AnalysisLog folder contains the HTML, text, XML, and JSON formats of the Analysis Report. If the malware severity is 3 and above, then it contains OpenIOC and STIX formats as well. You can identify these files by the malware file name. The malware file name is appended to _summary.html, _summary.json, _summary.txt, _summary.xml, _summary.ioc, and _summary.stix.xml.

The various sections of the HTML format of the Analysis Summary report are outlined here.



Threat Analysis Report

Summary

Threat Level	Malicious
File Name	[illegible]
MD5 Hash Identifier	[illegible]
SHA-1 Hash Identifier	[illegible]
SHA-256 Hash Identifier	[illegible]
File Size	[illegible] bytes
File Type	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
File Submitted	2015-07-21 [illegible]
Duration	[illegible] seconds
Sandbox Replication	[illegible] seconds
Screenshots	1

Engine Analysis

Engine	Threat Name	Severity
GTI File Reputation		
Gateway Anti-Malware		
Anti-Malware		
YARA		
Custom Rules		
Sandbox	Malware.Dynamic	High
Final		High

Behavior Classification

Exploiting, Shellcode	High
Spreading	Low
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	Low
Data spying, Sniffing, Keylogging, Ebanking Fraud	Low
Networking	Informational
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	Informational
Persistence, Installation Boot Survival	[illegible]

Dynamic Analysis

Action	Severity
Detected suspicious VBA content	High
Detected scripting content embedded in the sample	Low
[illegible]	Low
Installed low level keyboard hook procedure	Low
Set hook procedure to control system activities	Low
Created named mutex object	Low
Updated security descriptor for newly created process	Low
Modified Windows System Policy registry's settings	Low
Changed the protection attribute of the process	Informational
Retrieved the name of the network resource associated with a local device	Informational
Validated legacy of the software installation	Informational

Processes Analyzed

Name	Reason	Severity
[illegible]	loaded by MATD Analyzer	High

Embedded/Dropped content

MD5	Name
[illegible]	[illegible]

* Attachment was extracted from the sample file and stored in the dropfiles.zip

Screenshots

Note: a pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample

- Images: 1

[illegible]

- Run-Time DLLs: 24
- File Operations: 21
- Registry Operations: 571
- Process Operations: 16
- Network Operations: 1
- Other Operations: 12

Analysis Environment

Microsoft Windows 7 Service Pack 1 (build 7601, version 6.1.7601), 64-bit
Internet Explorer version: 9
Microsoft Office version: 2010
PDF Reader version: 10.0
No Flash player installed
No Flash player plugin installed
Platform Version 3.4.8.[illegible]

Figure 8-9 Threat Analysis Report

Table 8-7 Threat Analysis report sections

Item	Description
1	Summary. This section displays the details of the sample file. This includes the name, hash values, SHA-1 Hash identifier, file size in bytes and so on.
2	Engine Analysis section. This section provides the results from the analyzing methods used for the file. This section also displays the overall severity level for the file.
3	Behavior classification. This section provides the severity scores for various characteristics of a typical malware.

Table 8-7 Threat Analysis report sections *(continued)*

Item	Description
4	Dynamic Analysis section. This section displays the percentage of the file code that was executed. For example, the file might have taken an alternative path during execution due to which some part of the code was not executed at all. This section also provides a brief executive behavior summary with the corresponding severity levels. ● indicates a very low severity behavior. ● indicates a low severity behavior. ● indicates a medium severity behavior. ● indicates a high severity behavior. ● indicates a very high severity behavior.
5	Processes analyzed in this sample. This section lists all the files that were executed when dynamically analyzing the sample file. It also provides the reason how each file got to be executed along with their severity score. The Reason column indicates which other file or process created or opened this file. If there is only one file in the sample, the reason displayed is *loaded by MATD Analyzer*. If the sample file is a .zip file containing multiple files or if a file opens other files, the reason for the first file is *created by <file name> & loaded by MATD Analyzer*. For the subsequent files, the Reason column indicates all the files/processes that created it and all the files/processes that opened it. The Severity column indicates the severity level based on dynamic analysis for each file. • ○○○○○ — indicates a severity score of 0 and a threat level of informational. This is the severity for white-listed files. • ●○○○○ — indicates a severity score of 1 and a threat level of very low. • ●●○○○ — indicates a severity score of 2 and a threat level of low. • ●●●○○ — indicates a severity score of 3 and a threat level of medium. • ●●●●○ — indicates a severity score of 4 and a threat level of high. • ●●●●● — indicates a severity score of 5 and a threat level of very high. Click a file name to navigate to the section of the report that provides the details of the file behavior.
6	Embedded/Dropped content section. This section provides file name and MD5 hash value of all the files that were created by the samples during analysis
7	Screen-shots section. This section displays all the pop-up windows during dynamic analysis. By viewing these screenshots, you can determine if user intervention is required during dynamic analysis to know the actual behavior of the file. If user intervention is required, you can submit the file manually in user-interactive mode.
8	Operations details section. This section provides detailed information on all the operations performed by the sample file during dynamic analysis. These operations are grouped under corresponding groups. Expand each group for the specific operations. For example, expand **Files Operations** to view the files created, files deleted, files modified, files read, directories created or opened, directories removed, and so on.
9	Analysis Environment. This section includes the details of the analyzer VM, properties of the file, and so on

Analysis Results section

This is a section in the Threat Analysis report. In this section, you can view which methods reported that a sample file contains a malware.

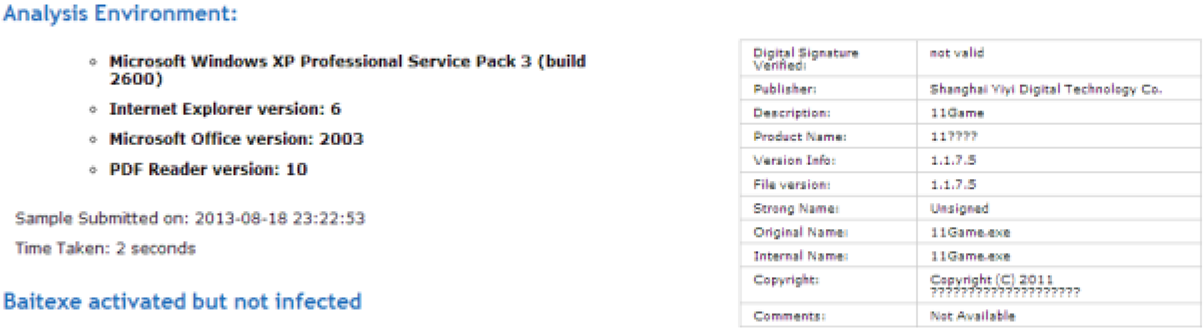
Table 8-8 Down Selector's Analysis

Label	Description
Engine	These are the possible methods that Advanced Threat Defense uses to analyze a file. • GTI File Reputation: Indicates McAfee GTI that is on the cloud. • Gateway Anti_Malware: Indicates McAfee Gateway Anti-Malware engine. • Anti-Malware: Indicates McAfee Anti-Malware Engine. • Sandbox: Indicates that the file was executed in an analyzer VM. Refer to the Analysis Environment section within the report to know the details of that VM.
Threat Name	Indicates the name for known malware in McAfee GTI, McAfee Gateway Anti-Malware engine, and McAfee Anti-Malware Engine.
Severity	Indicates the severity score from various methods. The highest severity score by a particular method is used to assign the final severity level for the sample.

Analysis Environment section

This is a section in the Threat Analysis report. You can find the following details in this section:

- Details of the corresponding analyzer VM such as the operating system, browser and version, and the applications and their versions installed on the analyzer VM.



Analysis Environment:

- Microsoft Windows XP Professional Service Pack 3 (build 2600)
- Internet Explorer version: 6
- Microsoft Office version: 2003
- PDF Reader version: 10

Sample Submitted on: 2013-08-18 23:22:53

Time Taken: 2 seconds

Baitexe activated but not infected

Digital Signature Verified:	not valid
Publisher:	Shanghai Yiyi Digital Technology Co.
Description:	11Game
Product Name:	11????
Version Info:	1.1.7.5
File version:	1.1.7.5
Strong Name:	Unsigned
Original Name:	11Game.exe
Internal Name:	11Game.exe
Copyright:	Copyright (C) 2011 ????????????????????
Comments:	Not Available

Figure 8-10 Analysis Environment section

- The time when the sample was submitted as per Advanced Threat Defense Appliance's clock.
- The time taken to analyze the file and generate the reports.
- On the right-hand side, a table provides the properties of the file. This includes information such as:
  - Signed or unsigned for the digital signature of the file.
  - Publisher's name if available.
  - Version details
  - Original name of the file so that you can search other sources such as the web.
- *Baitexe* process infected or not. At the end of each analysis Advanced Threat Defense creates an additional bait process called Baitexe. This Baitexe program calls two APIs (beep and sleep) only continuously. If this Baitexe process is infected by the previously executed sample, the behavior of Baitexe is different. In this case, a message *Baitexe activated and infected* is displayed. If the Baitexe process is not infected at all, the message *Baitexe activated but not infected* is displayed.

Behavior classification section

This is a section in the Threat Analysis report, which provides the severity scores for various characteristics of a typical malware.

Table 8-9 Behavior classification section

Label	Description
Persistence, Installation Boot Survival	Some malware have the capability to remain on the infected host. This is referred to as persistence. Installation boot survival refers to the capability of the malware to sustain even after a restart.
Hiding, Camouflage, Stealthness, Detection and Removal Protection	This refers to the capability of the malware to evade detection and removal.
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	This refers to the capability of the malware to bypass or mislead detecting methods and engines. Some malware has anti-disassembly code, which can confuse or delay malware analysis. Some malware attempt to determine if they are being executed in a sandbox. If true, they might take a different execution path. This score indicates the presence of such code in the malware.
Spreading	Indicates the capability of the malware to spread across the network.
Exploiting, Shellcode	Indicates the presence of shellcode that can exploit a running program.
Networking	Indicates the network-related behavior of the malware during dynamic analysis. For example, the malware might have triggered DNS queries or created sockets. If there is a severity score provided for this characteristic, correlate with the Network Operations details for the files in the sample.
Data spying, Sniffing, Keylogging, Ebanking Fraud	Indicates if the malware is capable of any such behaviors.

Operations details section

This section provides the details of every operation performed by a file during dynamic analysis. Separate sections are provided for every file that was executed as part of the sample.

- Run-time DLLs: Lists all the DLLs and their paths that were called by a file in runtime.
- File operations: Lists file operation activities like creation, open, query, modification, copy, move, deletion, and directory creation/deletion operations. This section also lists the file attributes and the MD5 hash value for the files.
- Registry operations: Provides the details of Windows registry operation activities like creation/open, deletion, modification, and query on registry sub-key and key entry.
- Process operations: Details the process operation activities such as new process creation, termination, new service creation, and code injection into other processes.
- Networking operations: Details networking operations such as DNS queries, TCP socket activities, and HTTP file download.
- Other operations: Provides details of operations not belonging to these categories. Examples are mutex signally objects, getting the system metric and configuration data of the analyzer VM.

Dropped files report

You can download a .zip file containing all the files that the sample created or touched during dynamic analysis. You can download these files using one of the following methods.

- In the **Analysis Results** page (**Analysis** | **Analysis Results**), click and select **Dropped Files**. Download the dropfiles.zip file, which contains the files that the sample created in the sandbox. To use this option, you must have enabled the **Dropped Files** option in the corresponding analyzer profile.
- After you click , select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same dropfiles.zip inside the AnalysisLog folder. The Complete Results contains the dropfiles.zip regardless of whether you have enabled **Dropped Files** option in the corresponding analyzer profile.

Disassembly Results

The Disassembly Results report provides the disassembly output listing for Portable Executable (PE) files. This report is generated based on the sample file after the unpacking process has completed. It provides detail information about the malware file such as, the PE header information.

The Disassembly Results report includes the following information:

- Date and time of the creation of the sample file
- File PE and Optional Header information
- Different section headers information
- The Intel disassembly listing

You can view the Disassembly Results report in the Advanced Threat Defense web application or download it as a file to your client computer. The contents of the report are the same in both the methods.

- To view the Disassembly Results report in the Advanced Threat Defense web application, select **Analysis** | **Analysis Results**. In the **Analysis Results** page, click and select **Disassembly Results**. To use this option, you must have enabled the **Disassembly Results** option in the corresponding analyzer profile.
- To download the report as a file, click in the **Analysis Results** page and select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains a file named as <file name>_detail.asm in the AnalysisLog folder. The Zip Report contains this .asm file regardless of whether you have enabled **Disassembly Results** option in the corresponding analyzer profile.

The Disassembly Results report provides the assembler instructions along with any static standard library call names like printf and Windows system DLL API call names embedded in the listing. If the global variables such as string text are referenced in the code, these string texts are also listed.

Table 8-10 A section of a sample Disassembly Results report

Column 1	Column 2	Column 3
:00401010	e8 1f2c0000	call 00403c34 ;;call URLDownloadToFileA

The virtual address of the instruction is shown in column 1, the binary instruction in column 2, and the assembly instruction with comments is in column 3. In the preceding example the `call 00403c34` instruction at memory location of `00401010` is making a functional call at `0x403c34` memory location, which is determined to be system DLL API function call determined to be `URLDownloadToFileA()`. The comment shown with the `;;` in this listing provides the library function name.

Logic Path Graph

This report is a graphical representation of cross-reference of function calls discovered during dynamic analysis. This report enables you to view the subroutines in the analyzed file that were executed during the dynamic analysis as well as the ones that were potentially not executed. These non-executed functions could be a potential time-bomb waiting to trigger under the right conditions.

The Logic Path Graph report is available as a Graph Modeling Language (GML) file. This file is an ASCII plain text format, which contains a graphical representation of the logic execution path of the sample in the GML (Graph Modeling Language) format. You cannot directly view this file in the Advanced Threat Defense web application, but download it to your client computer. Then you must use a graphical layout editor, like yWorks yEd Graph Editor, that supports GML format. You can use such an editor to display the cross-reference of all functions using this file as an input.

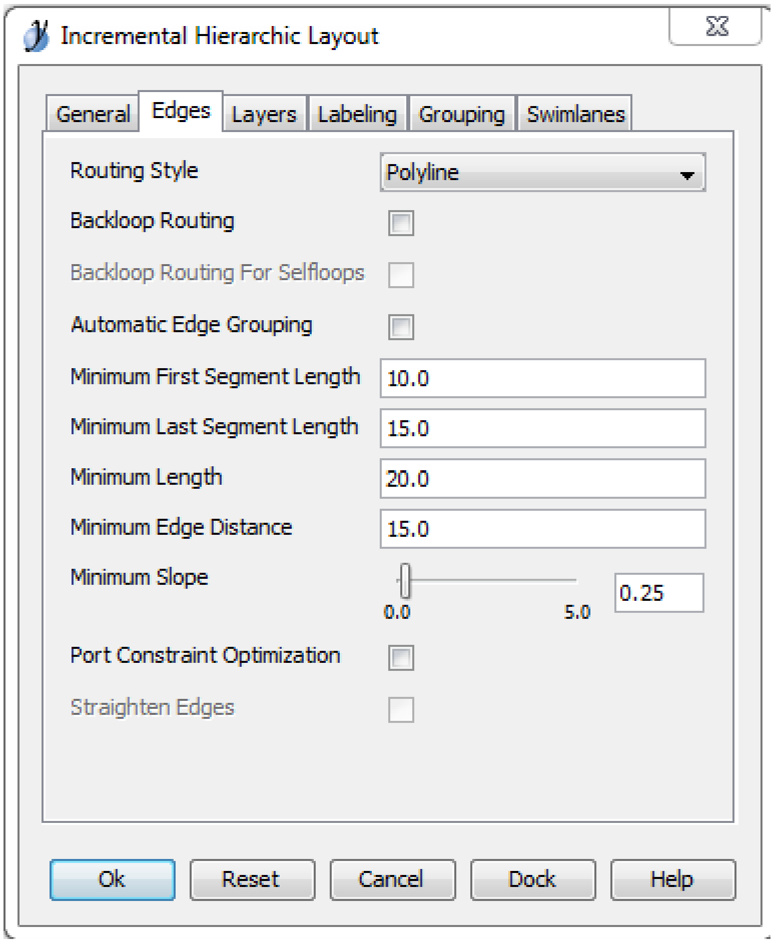
You can download the Logic Path Graph file using one of the following methods.

- In the **Analysis Results** page (**Analysis** | **Analysis Results**), click 📄 and select **Logic Path Graph**. Then download the <file name>_logicpath.gml file. To use this option, you must have enabled the **Logic Path Graph** option in the corresponding analyzer profile.

- After you click 📄, select **Complete Results**. Download the <sample_name>.zip file. This .zip file contains the same <file name>_logicpath.gml file in the AnalysisLog folder. The Zip Report contains the <file name>_logicpath.gml file regardless of whether you have enabled **Logic Path Graph** option in the corresponding analyzer profile.

This section uses yWorks yEd Graph Editor to explain how to use the Logic Path Graph GML file. In the yEd Graph Editor, you must first set the Routing Style. You need to do this only once, and this setting is saved for further use.

1. In the yEd Graph Editor, select **Layout** | **Hierarchical**.
2. In the **Incremental Hierarchic Layout** dialog, select the **Edges** tab and select **Polyline** from the **Routing Style** drop-down list.

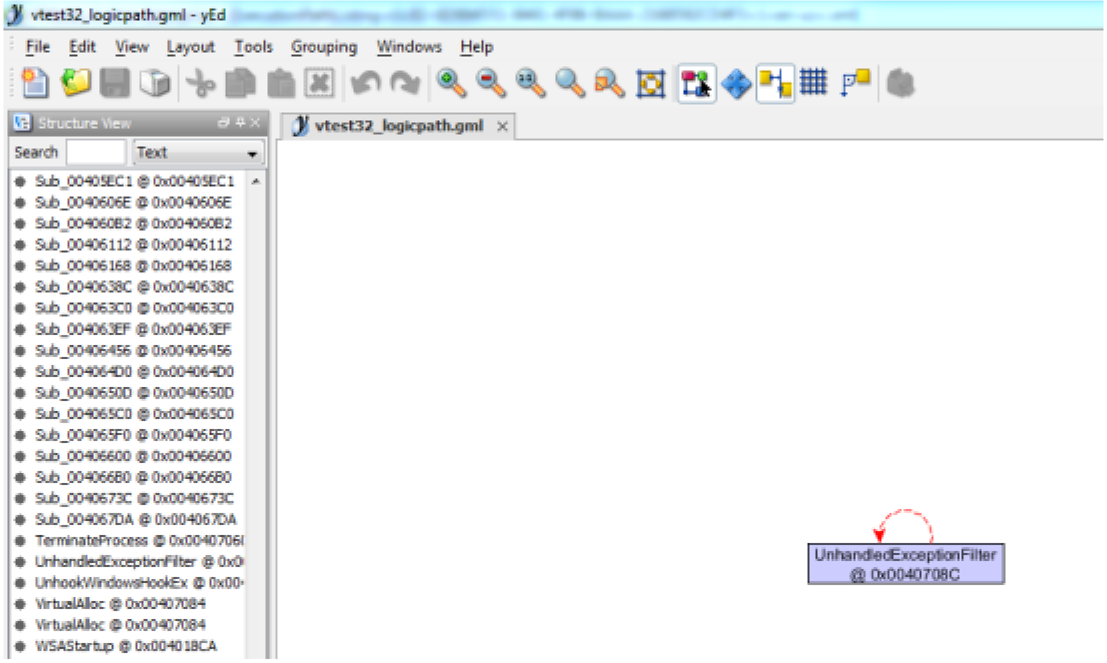


Routing Style: Polyline
Backloop Routing □
Backloop Routing For Selfloops □
Automatic Edge Grouping □
Minimum First Segment Length: 10.0
Minimum Last Segment Length: 15.0
Minimum Length: 20.0
Minimum Edge Distance: 15.0
Minimum Slope: 0.0 – 5.0: 0.25
Port Constraint Optimization □
Straighten Edges □

Figure 8-11 Configuring Routing Style in yEd Graph Editor

3. Click **Ok**.

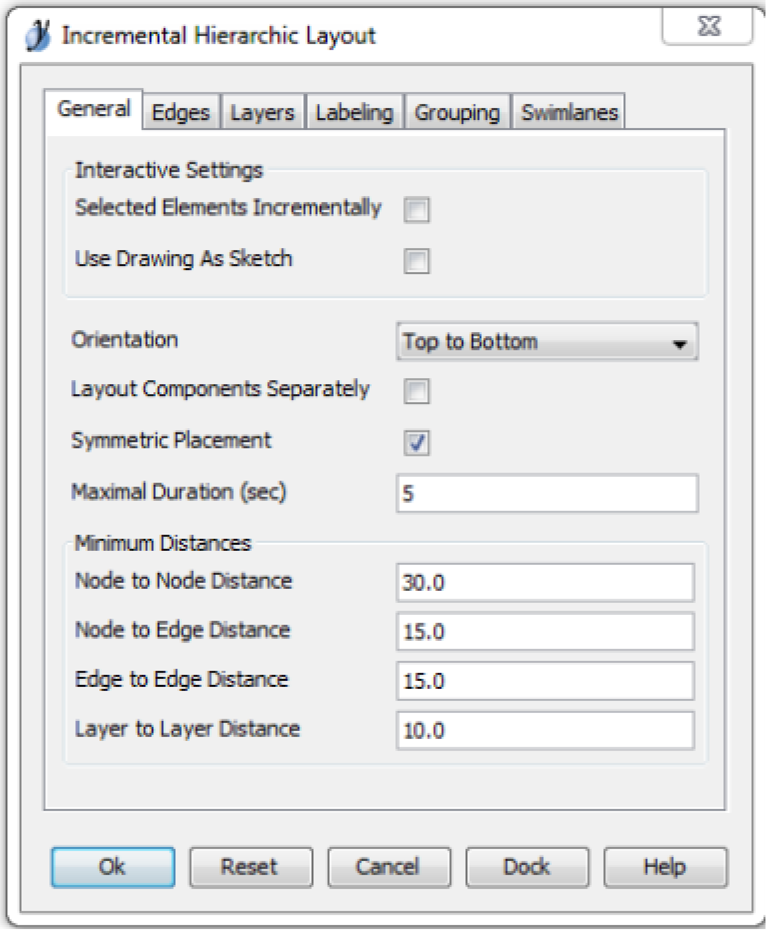
When you open the <file name>_logicpath.gml file in yEd Graph Editor, initially you might see many rectangle boxes overlapping each other or a single rectangle box as shown in the following example.



- Sub_00405EC1 @ 0x00405EC1
- Sub_0040606E @ 0x0040606E
- Sub_004060B2 @ 0x004060B2
- Sub_00406112 @ 0x00406112
- Sub_00406168 @ 0x00406168
- Sub_0040638C @ 0x0040638C
- Sub_004063C0 @ 0x004063C0
- Sub_004063EF @ 0x004063EF
- Sub_00406456 @ 0x00406456
- Sub_004064D0 @ 0x004064D0
- Sub_0040650D @ 0x0040650D
- Sub_004065C0 @ 0x004065C0
- Sub_004065F0 @ 0x004065F0
- Sub_00406600 @ 0x00406600
- Sub_004066B0 @ 0x004066B0
- Sub_0040673C @ 0x0040673C
- Sub_004067DA @ 0x004067DA
- TerminateProcess @ 0x0040706
- UnhandledExceptionFilter @ 0x0
- UnhookWindowsHookEx @ 0x00
- VirtualAlloc @ 0x00407084
- VirtualAlloc @ 0x00407084
- WSAStartup @ 0x004018CA

Figure 8-12 Open <file name>_logicpath.gml file

In the yEd Graph Editor select **Layout** | **Hierarchical.**



Interactive Settings

Selected Elements Incrementally □

Use Drawing As Sketch □

Orientation: Top to Bottom

Layout Components Separately □

Symmetric Placement ☑

Maximal Duration (sec): 5

Minimum Distances

Node to Node Distance: 30.0

Node to Edge Distance: 15.0

Edge to Edge Distance: 15.0

Layer to Layer Distance: 10.0

Figure 8-13 Incremental Hierarchic Layout dialog

In the **Incremental Hierarchic Layout** dialog, click **Ok** without changing any of the default settings. The following example shows the complete layout of the relationship of all subroutines detected during static disassembly processed.

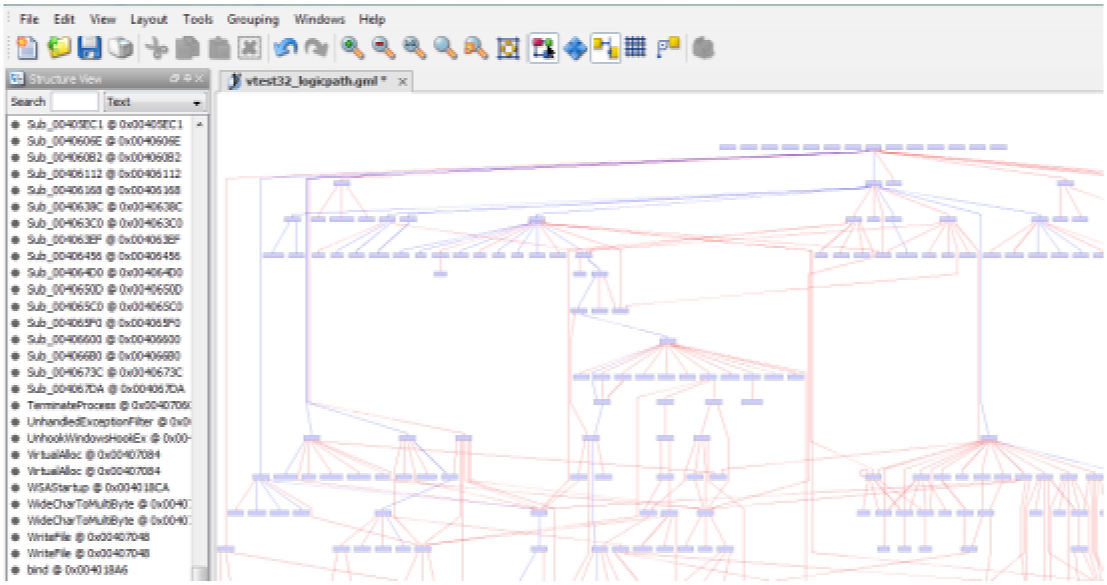

File
Edit
View
Layout
Tools
Grouping
Windows
Help
Structure View
Search
Text
vtest32_logicpath.gml *
Sub_00405EC1 @ 0x00405EC1
Sub_0040606E @ 0x0040606E
Sub_004060B2 @ 0x004060B2
Sub_00406112 @ 0x00406112
Sub_00406168 @ 0x00406168
Sub_0040638C @ 0x0040638C
Sub_004063C0 @ 0x004063C0
Sub_004063EF @ 0x004063EF
Sub_00406456 @ 0x00406456
Sub_004064D0 @ 0x004064D0
Sub_0040650D @ 0x0040650D
Sub_004065C0 @ 0x004065C0
Sub_004065F0 @ 0x004065F0
Sub_00406600 @ 0x00406600
Sub_004066B0 @ 0x004066B0
Sub_0040673C @ 0x0040673C
Sub_004067DA @ 0x004067DA
TerminateProcess @ 0x0040706
UnhandledExceptionFilter @ 0x0
UnhookWindowsHookEx @ 0x00
VirtualAlloc @ 0x00407084
VirtualAlloc @ 0x00407084
WSAStartup @ 0x004018CA
WideCharToMultiByte @ 0x0040
WideCharToMultiByte @ 0x0040
WriteFile @ 0x00407048
WriteFile @ 0x00407048
bind @ 0x004018A6

Figure 8-14 Layout of the subroutines relationships

The graph depicts an overview of the complexity of the sample as seen by the cross-reference of function calls. The following shows more detail on the function names and their addresses as seen by zooming in.

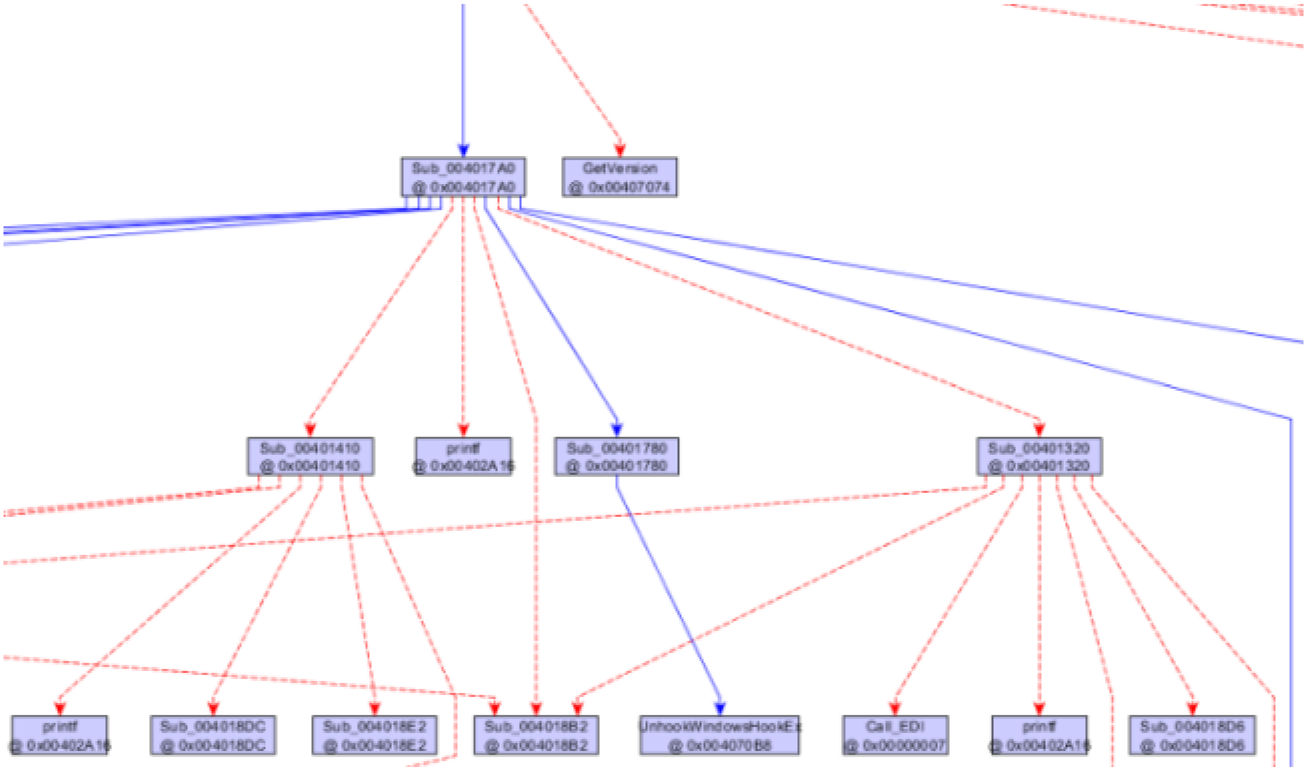

Sub_004017A0 @ 0x004017A0
GetVersion @ 0x00407074
Sub_00401410 @ 0x00401410
printf @ 0x00402A16
Sub_00401780 @ 0x00401780
Sub_00401320 @ 0x00401320
printf @ 0x00402A16
Sub_004018DC @ 0x004018DC
Sub_004018E2 @ 0x004018E2
Sub_004018B2 @ 0x004018B2
UnhookWindowsHookEx @ 0x004070B8
Call_EDI @ 0x00000007
printf @ 0x00402A16
Sub_004018D6 @ 0x004018D6

Figure 8-15 Zoom in on the layout

Two colors are used to indicate the executed path. The red dash lines show the non-executed path, and the blue solid lines show the executed path.

According to the preceding control graph, the subroutine (Sub_004017A0) at virtual address 0x004017A0 was executed and is shown with a blue solid line pointing to the Sub_004017A0 box. However, the subroutine (GetVersion]) was not called potentially as there is a red dash line pointing to it.

The Sub_004017A0 subroutine is making 11 calls as there are 11 lines coming out of this box. Seven of these 11 calls were executed during dynamic analysis. One of them is calling Sub_00401780 as there is a blue solid line pointing from Sub_004017A0 to Sub_00401780. Calls to Sub_00401410, printf, Sub_00401882, and Sub_00401320 were not executed and shown with red dashed line pointing at them.

The Sub_00401780 subroutine is making only one unique call as there is only one line coming out from this box. This call was executed during dynamic analysis.

User API Log

The User API Logs are contained in various files.

- The .log file contains the Windows user-level DLL API calls made directly by the analyzed file during dynamic analysis. To view this file in the Advanced Threat Defense web application, select **Analysis** | **Analysis Results.** Then click 📄 and select **User API Log.** Alternatively, click 📄, select **Complete Results.** Download the <sample_name>.zip file. This .zip file contains the same information in the <sample name>.log file in the AnalysisLog folder. The content of the .log file includes the following:
  - A record of all systems DLL API calling sequence.
  - An address which indicates the approximate calling address where the DLL API call was made.
  - Optional input and output parameters, and return code for key systems DLL API calls.
- The following are the other files containing the dynamic execution logs. All these files are contained in the <sample name>.zip file.
  - <sample name>ntv.txt file. This file contains the Windows Zw version of native system services API calling sequence during the dynamic analysis. The API name typically starts with Zw as in ZwCreateFile.
  - log.zip
  - dump.zip
  - dropfiles.zip
  - networkdrive.zip

Download the complete results .zip file

Advanced Threat Defense produces detailed analysis for each submitted sample. All the available reports for an analyzed sample are available in a .zip file, which you can download from the Advanced Threat Defense web application.

Task

1. Select **Analysis** | **Analysis Results.**
2. In the **Analysis Results** page, click 📄 and select **Complete Results** .

   Download the <sample_name>.zip file to the location you want. This .zip file contains the reports for each analysis. The files in this .zip file are created and stored with a standard naming convention. Consider that the sample submitted is vtest32.exe. Then the .zip file contains the following results:

- vtest32_summary.html (.json, .txt, .xml) — This is the same as the Analysis Summary report. There are four file formats for the same summary report in the .zip file. The html and txt files are mainly for end users to review the analysis report. The .json and .xml files provide well-known malware behavior tags for high-level programming script to extract key information.

  If the malware severity is 3 and above, then it contains .ioc, and .stix.xml formats of the Analysis Summary report for the sample.

- vtest32.log — This file captures the Windows user-level DLL API calling activities during dynamic analysis. You must thoroughly examine this file to understand the complete API calling sequence as well as the input and output parameters. This is the same as the User API Log report.

- vtest32ntv.txt — This file captures the Windows native services API calling activities during dynamic analysis.

- vtest32.txt — This file shows the PE header information of the submitted sample.

- vtest32_detail.asm — This is the same as the Disassembly Results report. This file contains reverse-engineering disassembly listing of the sample after it has been unpacked or decrypted.

- vtest32_logicpath.gml — This file is the graphical representation of cross-reference of function calls discovered during dynamic analysis. This is the same as the Logic Path Graph report.

- log.zip —This file contains all the run-time log files for all processes affected by the sample during the dynamic analysis. If the sample generates any console output text, the output text message is captured in the ConsoleOutput.log file zipped up in the log.zip file. Use any regular unzip utility to see the content of all files inside this log.zip file.

- dump.zip — This file contains the memory dump (dump.bin) of binary code of the sample during dynamic analysis. This file is password protected. The password is *virus*.

- dropfiles.zip — This is the same as the Dropped Files report in the **Analysis Results** page. The dropfiles.zip file contains all files created or touched by the sample during the dynamic analysis. It is also password protected. The password is *virus*.

> ℹ Advanced Threat Defense does not provide you access to the original sample files that it analyzed. If Network Security Platform is integrated, you can use the **Save File** option in the Advanced Malware policy to archive samples. However, note that the Sensor's simultaneous file scan capacity is reduced if the **Save File** option is enabled. See the latest *Network Security Platform IPS Administration Guide* for the details.

Download the original sample

Advanced Threat Defense allows user to download the originally submitted files. All the submitted samples are available in a .zip file, which you can download by following below steps.

Task

1 Select **Manage** | **User Management**.

2 In the **User Management** page, select your user profile.

3 Enable **Sample Download** option.

4 Select **Analysis Results**, click **Reports** icon and select **Original Sample**.

5 Save the zipped **<SAMPLENAME>_<MD5SUMOFSAMPLE>.zip** file on your local machine

6 Extract the content of **<SAMPLENAME>_<MD5SUMOFSAMPLE>.zip** using `infected` as password.

Working with the Advanced Threat Defense Dashboard

When you access Advanced Threat Defense from a client browser, the Advanced Threat Defense Dashboard is displayed. You can view the following monitors on the Advanced Threat Defense Dashboard:

- VM Creation Status — Shows the status for analyzer VMs that being created.
- File Counters — Indicates the number of samples in progress. The indicated samples displayed in **Running** count are either being processed by various engines, heuristic analysis, or sandbox processing.

  > ℹ The number of samples displayed in **Running** count include all of the pre-processors and may indicate a value larger than the configured number of sandboxes.

- Top 5 URLs Analyzed by GTI — Lists five most severe URLs being analyzed by GTI.
- Top 5 URLs — Lists five most severe URLs being analyzed.
- VM Profile Usage — Lists the number of files analyzed by VMs along with number of licenses for these analyzer VMs.
- Files Analyzed by Engine — Provides the severity and number of files analyzed by GAM, GTI and Sandbox.
- Top 10 File Types by volume — Provides a view of ten most number of files of different types being analyzed.
- Top 5 Recent Malware by Filename — Lists five most severe malware files in your network by file name.
- Top 10 Malware by Threat Name — Lists ten most severe malware files in your network by threat name.
- System Health — Provides the system health details of the Advanced Threat Defense Appliance.
- System Information — Provides the version numbers for the software components of Advanced Threat Defense Appliance.

Task

1. Click **Dashboard** to view the monitors.
2. Specify the criteria for the data to be displayed in the monitors.
   a. Specify the time period for the information to be displayed in the monitors.

      For example, you can select to view the information for the past one hour. By default, data for the past 14 days is shown. This field does not affect the System Health and System Information monitors.

   b. To refresh the monitors now, click ⟳.

c Click ✎ to edit the dashboard settings.

Table 8-11 Dashboard settings

Option	Definition
Monitors	Select the monitors that you want to see on the Dashboard.
Automatic Refresh	Set the frequency at which the Dashboard should automatically refresh itself. 💡 If you want to refresh the dashboard only manually, select **Disabled**. When required to refresh the Dashboard, click ⟳. This enables you to view the snapshot of the Dashboard at a specific point in time.
Layout	Specify the number of columns into which you want to organize the Dashboard.
OK	Click to save and apply the Dashboard settings.
Cancel	Click to retain the last saved settings.

d Click 💾 to save the dashboard settings.

3 Optionally, set the display settings for each monitor.

- To collapse a monitor, click ︽
- To hide a monitor, click ✕
- To change the display format of a monitor, click ⚙

Malware analysis monitors

The following are the monitors related to malware analysis.

File Counters

This monitor shows the analysis status for files submitted during the specified time period. For example, if you set the time period for the data in the dashboard as last 5 minutes, this monitor shows the count of files in completed, analyzing, and waiting statuses since the last 5 minutes. If you view this monitor in the stacked bar chart format, it also displays the severity level for the files.

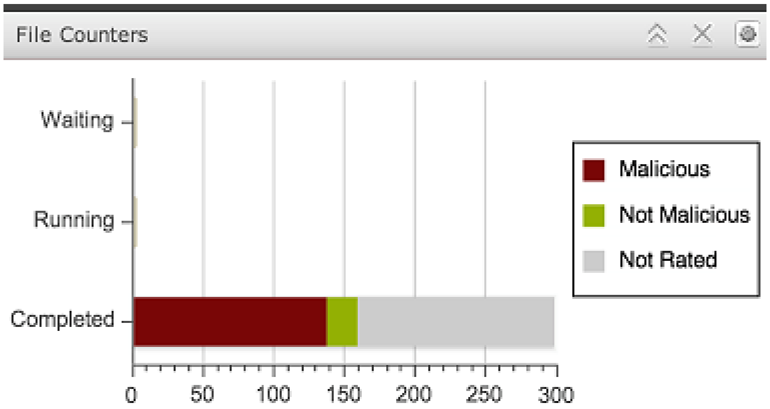


Figure 8-16 File Counters monitor

- The severity levels are indicated using various colors.
- To hide the files for a particular severity, click the corresponding severity in the legend. For example, if you want to focus on only the malicious files, click **Not Malicious** and **Not Rated** in the legend. Now the chart shows only the high-severity malware that is in the waiting, running, and completed statuses. Click again on **Not Malicious** and **Not Rated** to view the combined chart.
- Move the mouse over a particular block in the chart to view the number of files that make up that block.

This monitor has drill - down capabilties. Once you click the mouse over a particular block, Advanced Threat Defense takes you to **Analysis Results** page, displaying the records sorted as per the chosen block.

Top 10 File Types by Volume

This monitor shows the count of top 10 file types based on their volume. In the tabular format, it shows the percentage for each type. In the chart, it also shows the count of malicious, not malicious and not rated files.

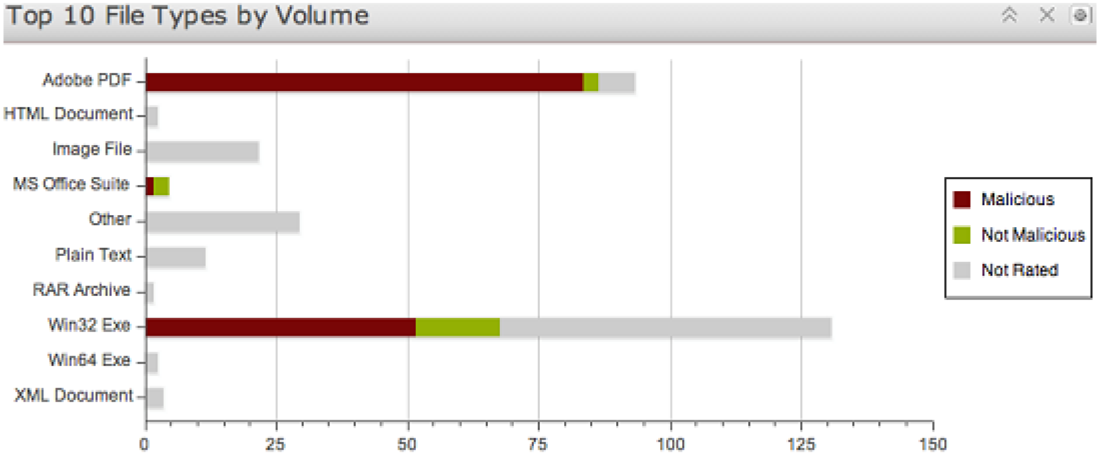


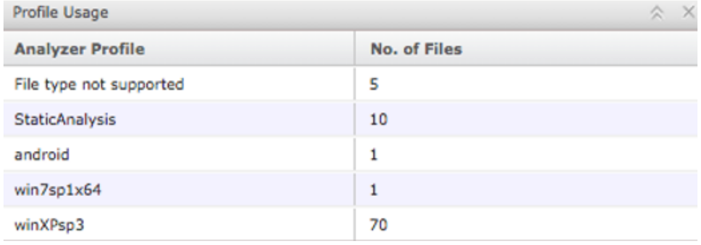
Figure 8-17 Top 10 File Types by volume monitor

- The malicious, not malicious and not rated file counts are indicated using different colors.
- To hide the malicious or not malicious files, click the corresponding severity level in the legend.
- Move the mouse over a particular block in the chart to view the number of files that make up that block.

This monitor has drill - down capabilties. Once you click the mouse over a particular block, Advanced Threat Defense takes you to **Analysis Results** page, displaying the records sorted as per the chosen block.

Profile Usage

This monitor shows the number of times each analyzer profile has been used for analyzing files.


Profile Usage

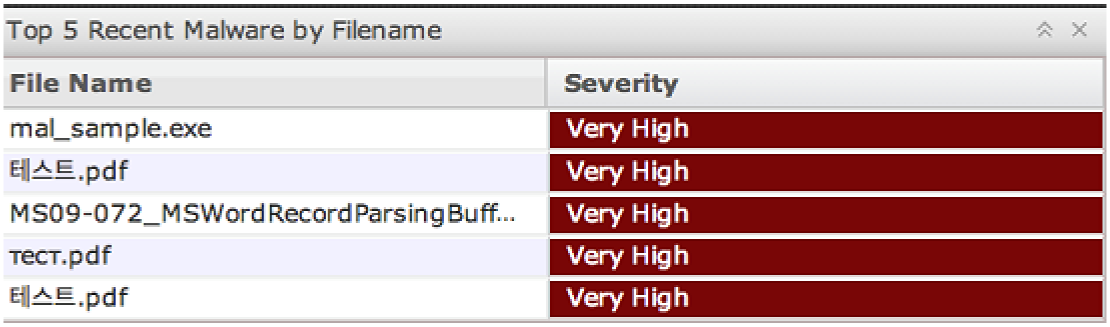
Analyzer Profile	No. of Files
File type not supported	5
StaticAnalysis	10
android	1
win7sp1x64	1
winXPsp3	70

Figure 8-18 Analyzer Profile Usage monitor

Top 5 Recent Malware by File Name

In this monitor, you can view the names of five malicious files detected in your network with the most severe ones listed on top. This information might enable further research such as finding more information about these files on the web.

- The listed malware files are sorted based on their severity level in the descending order.
- The first column displays the file names. The second column displays the severity level.



Top 5 Recent Malware by Filename

File Name	Severity
mal_sample.exe	Very High
테스트.pdf	Very High
MS09-072_MSWordRecordParsingBuff...	Very High
тест.pdf	Very High
테스트.pdf	Very High

Figure 8-19 Top 5 Recent Malware by File Name monitor

Top 10 Malware by Threat Name

In this monitor, you can view the names of ten most severe malware files in your network by threat name.

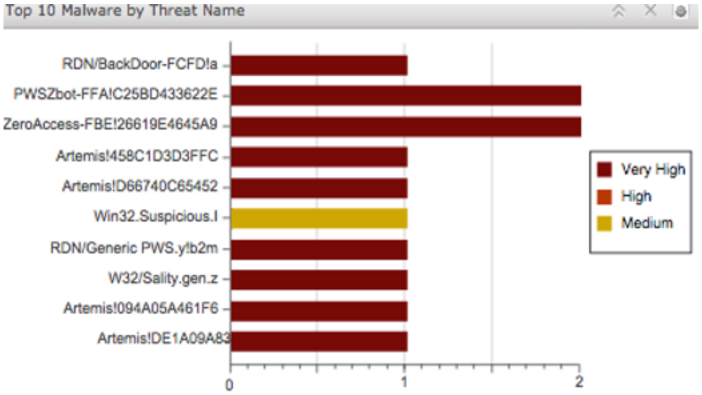


Figure 8-20 Top 10 Malware by Threat Name

This monitor has drill - down capabilties. Once you click the mouse over a particular block, Advanced Threat Defense takes you to **Analysis Results** page, displaying the records sorted as per the chosen block.

Files Analyzed by Engine

In this monitor, you can view the severity and number of files analyzed by GAM, GTI and Sandbox.

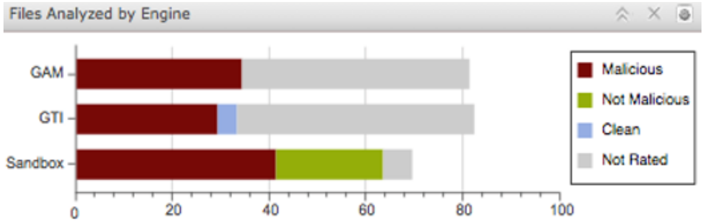


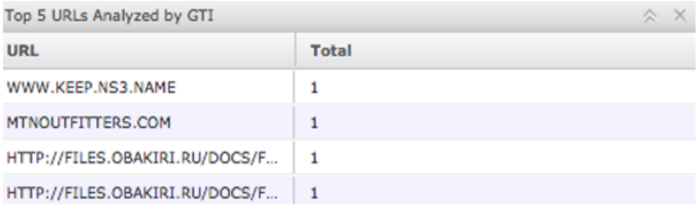
Figure 8-21 Files Analyzed by Engine

> This monitor has drill - down capabilties. Once you click the mouse over a particular block, Advanced Threat Defense takes you to **Analysis Results** page, displaying the records sorted as per the chosen block.

Top 5 URLs Analyzed by GTI

In this monitor, you can view the names of five most severe URLs being analyzed by GTI. This information might enable further research such as finding more information about these files on the web.

- The listed malware files are sorted based on their severity level in the descending order.
- The first column displays the file names. The second column displays the severity level.



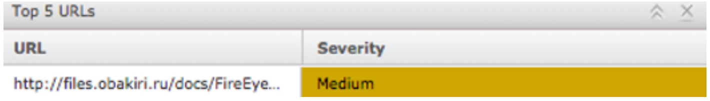
URL	Total
WWW.KEEP.NS3.NAME	1
MTNOUTFITTERS.COM	1
HTTP://FILES.OBAKIRI.RU/DOCS/F...	1
HTTP://FILES.OBAKIRI.RU/DOCS/F...	1

Figure 8-22 Top 5 URLs Analyzed by GTI

Top 5 URLs

In this monitor, you can view the names of five malicious files detected in your network with the most severe ones listed on top. This information might enable further research such as finding more information about these files on the web.

- The listed malware files are sorted based on their severity level in the descending order.
- The first column displays the file names. The second column displays the severity level.



URL	Severity
http://files.obakiri.ru/docs/FireEye...	Medium

Figure 8-23 Top 5 URLs

VM Creation Status monitor

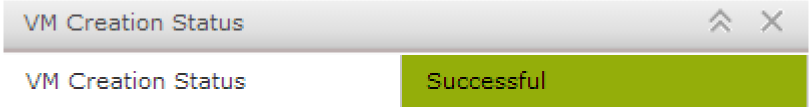
This monitor displays the color based on the status of VM creation. Below is the color code followed:

In Progress - Yellow

Failed - Red

Success - Green

Below is an example of **VM Creation Status monitor** when the status of VM creation is "Success" :



VM Creation Status

VM Creation Status	Successful

Figure 8-24 VM Creation Status monitor

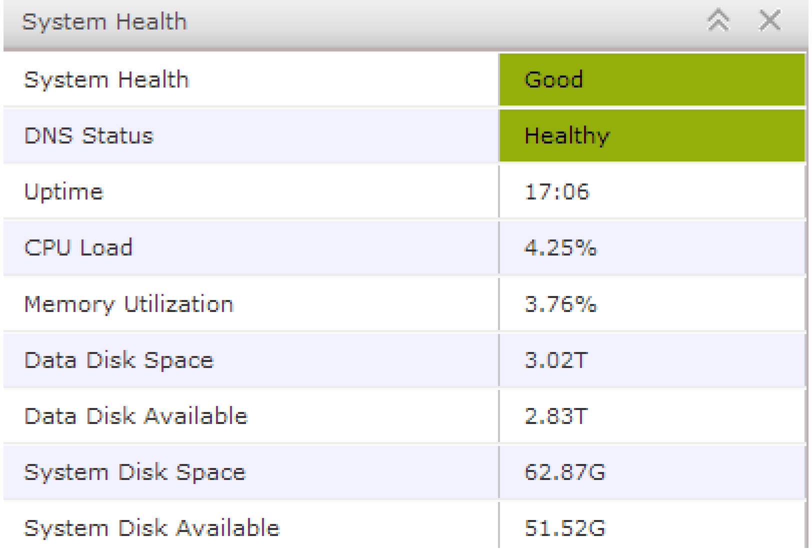
Advanced Threat Defense performance monitors

The following are the monitors related to Advanced Threat Defense Appliance performance.

System Health

This monitor displays the health of the Advanced Threat Defense Appliance in a table.

- System Health — Indicates whether the system health is in good state. "Green" color indicates good health and "Red" color indicates bad health.
- DNS Status — Indicates the connection status between Advanced Threat Defense and the configured DNS servers. If Advanced Threat Defense is able to connect to the preferred and alternate DNS server, then the DNS Status is *Healthy* and the same is indicated by "Green" color. If Advanced Threat Defense is unable to connect to the preferred DNS server, the DNS Status is *critical* and the same is indicated by "Red " color. If Advanced Threat Defense is not connected to any preferred DNS server, the DNS Status is *Not Configured* and the same is indicated by "Red " color.
- Uptime — The number of hours the Appliance has been running continuously.
- CPU Load — The actual system load. For example, 100% CPU load indicates the CPU is fully loaded; 125% indicates that the CPU is fully loaded and 25% of the load is yet to be processed.
- Memory Utilization — The percentage of the Appliance's memory in use currently.
- Data Disk Space — The Appliance's disk capacity (in terabyte) for sample data storage such as the samples themselves and their report files.
- Data Disk Available — Disk space currently available (in terabyte) for sample data storage.



System Health

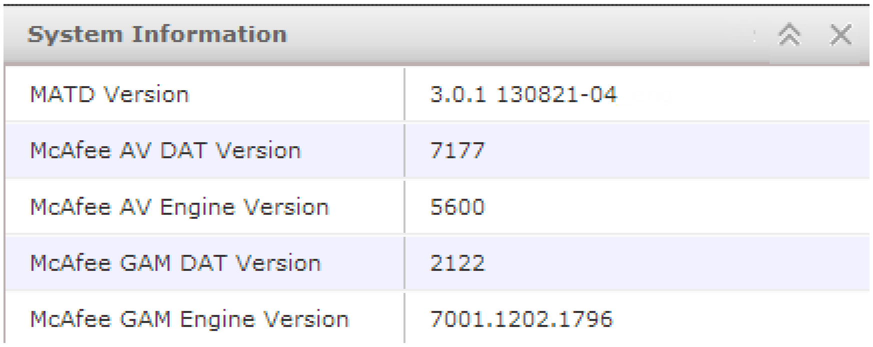
System Health	Good
DNS Status	Healthy
Uptime	17:06
CPU Load	4.25%
Memory Utilization	3.76%
Data Disk Space	3.02T
Data Disk Available	2.83T
System Disk Space	62.87G
System Disk Available	51.52G

Figure 8-25 System Health monitor

- System Disk Space — The Appliance's disk capacity for storing the Advanced Threat Defense system software data.
- System Disk Available — Disk space currently available for storing the Advanced Threat Defense system software data.

System Information

This monitor shows the version numbers of the software components related to Advanced Threat Defense.



System Information

MATD Version	3.0.1 130821-04
McAfee AV DAT Version	7177
McAfee AV Engine Version	5600
McAfee GAM DAT Version	2122
McAfee GAM Engine Version	7001.1202.1796

Figure 8-26 System Information monitor

9 Clustering McAfee Advanced Threat Defense Appliances

When you have a very heavy load of files to be analyzed for malicious content, you can cluster two or more McAfee Advanced Threat Defense Appliances. So, the analysis load is efficiently balanced between the McAfee Advanced Threat Defense Appliances (nodes) in the cluster.

Consider multiple inline Sensors submitting hundreds of files per second to one McAfee Advanced Threat Defense Appliance. In the blocking mode, a Sensor waits for up to 6 seconds for McAfee Advanced Threat Defense to analyze a file. After this time period, the Sensor forwards the file to the target endpoint. Faster response from McAfee Advanced Threat Defense could be accomplished by clustering McAfee Advanced Threat Defense Appliances for load-balancing.

Contents

Understanding Advanced Threat Defense cluster

Clustering Advanced Threat Defense Appliances is a feature, which is available from release 3.2.0. To create a cluster of Advanced Threat Defense Appliances, you need two or more functional Advanced Threat Defense Appliances. Among these Advanced Threat Defense Appliances, identify the Primary Advanced Threat Defense Appliance. All other Advanced Threat Defense Appliances act as the secondary. With release 3.4.2, a node which is in the same L2 network as Primary Advanced Threat Defense Appliance can be directly added as a Backup node, which takes over as Primary node if original Primary node is down. You use the web application of the Primary node to integrate these Advanced Threat Defense Appliances to form the cluster. Each Advanced Threat Defense Appliance in a cluster is referred to as a node.

The Primary node or the primary Advanced Threat Defense Appliance acts as the external interface for the cluster. That is, the Primary node is virtually associated to the IP address of the cluster from the standpoint of configuration and file submission. The integrated products and users access the primary node to submit files for analysis and retrieve the results and reports. The Primary node is also the template and control center for the cluster. It is responsible for load-balancing the files among all nodes and for retrieving the reports of analyzed files. If Backup node is present in cluster, then these integrated products need to be configured with cluster IP address.

As mentioned earlier, clustering Advanced Threat Defense Appliances serves to load-balance the files and provides a high-availability of secondary nodes.

> If the Primary node is down for some reason, the Backup node takes over the responsibilities of Primary node and becomes active taking the cluster IP address from Primary node. After revival, the Primary node waits as backup till the time the Backup node goes down. At any point of time, Backup node also receives and analyzes the samples like any other node.

Pre-requisites and considerations

- There can be a maximum of 10 nodes in a cluster including the primary node.
- You must use the eth-0 interfaces (management ports) of the Advanced Threat Defense Appliances for cluster communication. Also, for best performance, the eth-0 interfaces of all nodes must be in the same layer-2 of the OSI reference model.

  To locate the eth-0 interfaces in your Appliance, see Check your shipment on page 22.
- The nodes must be homogenous regarding the following:
  - Advanced Threat Defense software version. The software versions of all nodes must exactly match.
  - Analyzer VMs. All nodes must have the same analyzer VMs.

    > Before you configure the cluster, make sure the VM profiles are exactly the same in all the nodes of the cluster. All the settings in the VM profiles, including the VM profile name, must be the same across the nodes.
    >
    > When you create a new VM profile or modify an existing one after cluster-creation, recall that VM-profile-related changes are not propagated to all the nodes automatically. First, dismantle the cluster. Then manually make the exact change in each node. If you are creating a new VM profile, make sure you create this VM profile in all the nodes before you select this new VM profile in any of the analyzer profiles. If you need to modify an existing VM profile, make sure you immediately do the same modification in each node. Finally, recreate the cluster.
  - VM profiles on all nodes must exactly match.
  - It is recommended that DAT and engine versions of McAfee Anti-Malware Engine are the same in all nodes.
  - It is recommended that DAT and engine versions of McAfee Gateway Anti-Malware Engine are the same in all nodes.
- The nodes can be heterogenous regarding the following:
  - Hardware. That is, you can create a cluster using a combination of ATD-3000 and ATD-6000 Appliances.
  - FIPS compliance. Regardless of primary or secondary, some nodes can be in FIPS mode and the rest in non-FIPS mode.

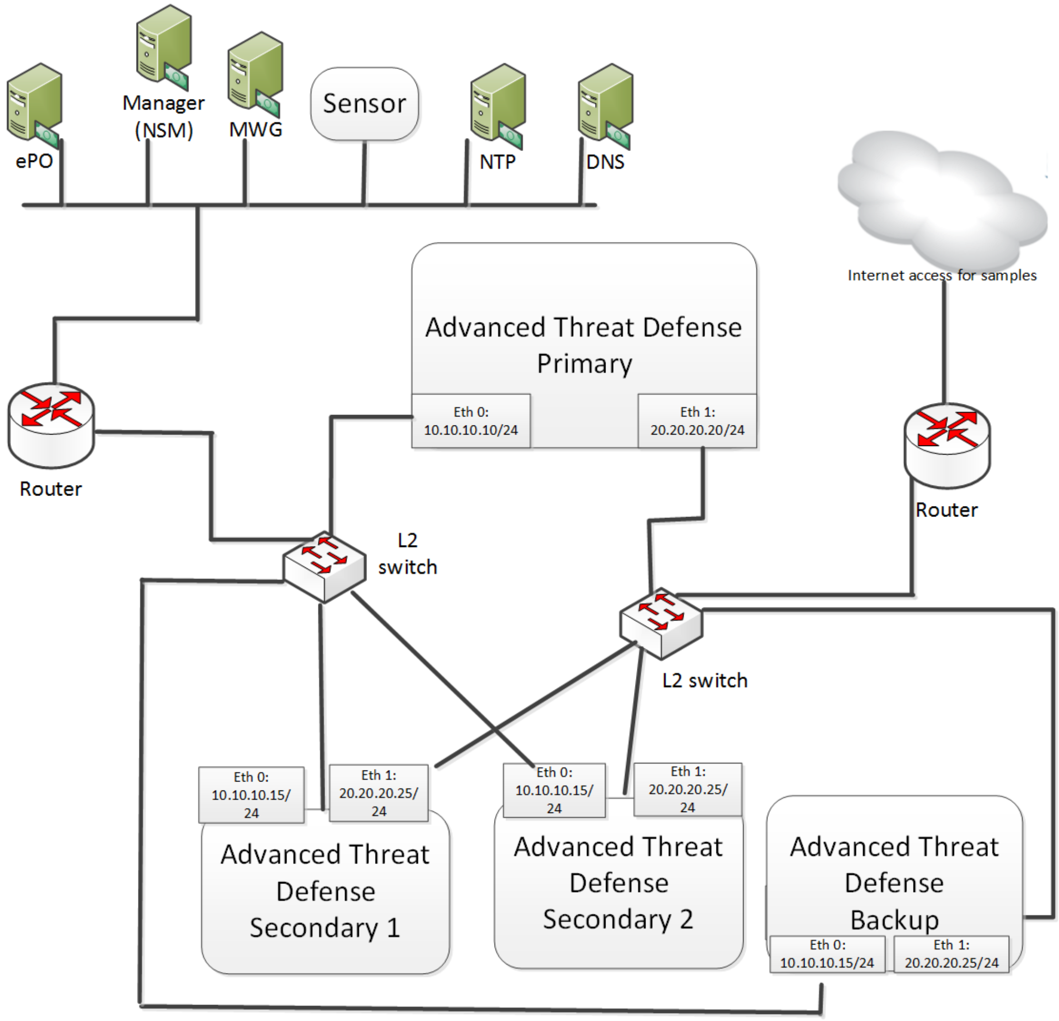
- Use the IP address of the Primary node to submit files and to integrate with other products such as Network Security Platform and Web Gateway. The Primary node or the primary Advanced Threat Defense Appliance acts as the external interface for the cluster. That is, the Primary node is virtually associated to the IP address of the cluster from the standpoint of configuration and file submission. If you integrate Network Security Platform, Web Gateway and Email Gateway with the secondary nodes, these nodes function like standalone Advanced Threat Defense Appliances. If Backup node is present in cluster, then these integrated products need to be configured with cluster IP address.

  Integrating an Advanced Threat Defense cluster with Email Gateway is supported with release 3.4.2.

- If the Primary node is down, the Backup node takes over. Backup node must be in same L2 network as Primary node.
- User can view the Analysis Status and Analysis Results of all the nodes in cluster from Active node, that is Primary node or Backup node.
- You can wipe out all cluster related configurations from a node and make it as a standalone box. `cluster withdraw` command is used to destroy cluster using CLI. It is permitted to run at all nodes (Primary/ Backup/Secondary). This command can be used in scenarios where normal means of removing a node (Remove Node/ Withdraw From Cluster) does not remove that node from cluster. See also cluster withdraw on page 349.

Network connections for an Advanced Threat Defense cluster

Figure 9-1 An example Advanced Threat Defense cluster deployment



In the example illustrated above, the eth-0 interfaces of all nodes are connected to the same switch (L2 network). Eth-0 interface of the primary acts as the management interface of the cluster whereas the eth-0 of the secondary and backup node are used to exchange information with the primary. The Backup node acts as a secondary node till the time the Primary node goes down for some reason and the Backup node assumes the active primary node role. The primary node load balances the files received on the eth-0 interface among the secondary nodes based on the number of files submitted to a node. A highly burdened node receives lesser number of samples for processing as opposed to a less burdened node. The primary node transfers files to be analyzed by the secondary node through the eth-0 interface and uses the same to retrieve results. When cluster configuration changes are made using the primary node, they are synchronized across the secondary nodes and the backup node through the eth-0 interface.

In this example, eth-1 is used to provide network access to malware running on the analyzer VMs. This isolates the network traffic generated by malware from the production network to which eth-0 interfaces are connected.

A local database is maintained at the Primary node which lists the MD5 hash value along with corresponding node-id of the samples blacklisted by Advanced Threat Defense. Node-id is the primary identifier of a node that processes a particular sample. Whenever a sample is submitted to Advanced Threat Defense, the Primary node looks for an existing entry of this sample in its newly created database. If the MD5 hash value of a sample matches with an existing one in the database, this previously blacklisted sample is sent to the node based on the corresponding node-id of the sample.

This approach ensures that every previously submitted, blacklisted sample reaches the node that analyzed it earlier, hence avoiding re-analysis of the blacklisted samples by any other node in the cluster.

Advanced Threat Defense determines the wait time for a submitted sample before it gets picked for analysis. The wait time is calculated based on the current sample analysis rate of the nodes. For samples submitted through MEG, a threshold wait time of 780 seconds is allotted. Advanced Threat Defense rejects all the incoming samples from MEG until the wait time drops below this threshold value.

How the Advanced Threat Defense cluster works?

Recall that when you cluster Advanced Threat Defense Appliances, the primary node acts as the template and control center for the entire cluster. After you define the cluster, you use the primary node to manage the configuration for the cluster.

> Backup node behaves as a secondary node for all configuration processes.

For the sake of explanation, the entire Advanced Threat Defense configuration can be classified as the following:

- Synchronized configuration — Certain configurations can only be done using the primary node. When you save these configurations, the primary node sends a snapshot of its current configuration as a file to all secondary nodes. The secondaries save these settings in their database. This synchronization process does not affect the file analysis capabilities of an Advanced Threat Defense Appliance.

  The primary node has the latest version of the configuration file. If the version of the configuration file does not match between the primary and a secondary node, the primary node pushes the configuration file automatically to that secondary.

  The following configurations are synchronized automatically between all nodes:

  - Analyzer profiles
  - User management
  - McAfee ePO/DXL integration details
  - Proxy Settings
  - DNS settings
  - System time based on the settings in the **Date and Time Settings** page. If you manually modify the time, the same is set on all nodes. If you configure NTP servers, the same NTP servers are used for all nodes. However, time zone is not synchronized.

  The web application pages for the configurations listed above are disabled in both secondary and Backup nodes.

- Unsynchronized configuration — The following are not synchronized automatically. Use the individual nodes to configure these.
  - Advanced Threat Defense software version.
  - Analyzer VMs.

    > Before you configure the cluster, make sure the VM profiles are exactly the same in all the nodes of the cluster. All the settings in the VM profiles, including the VM profile name, must be the same across the nodes.
    >
    > When you create a new VM profile or modify an existing one after cluster-creation, recall that VM-profile-related changes are not propagated to all the nodes automatically. First, dismantle the cluster. Then manually make the exact change in each node. If you are creating a new VM profile, make sure you create this VM profile in all the nodes before you select this new VM profile in any of the analyzer profiles. If you need to modify an existing VM profile, make sure you immediately do the same modification in each node. Finally, recreate the cluster.

  - VM profiles.
  - DAT and engine versions of McAfee Anti-Malware Engine.
  - DAT and engine versions of McAfee Gateway Anti-Malware Engine.
  - Whitelist and blacklist entries.
  - Time zone.
  - In a Advanced Threat Defense cluster setup, each node maintains its set of custom YARA rules. That is, the custom YARA rules that you define in the primary node are not sent to the secondary nodes automatically.

    > Configuration changes made through the CLI are not exchanged. Make the same changes in each node individually.

When treated as part of a cluster, the secondary nodes are transparent to users and integrated products.

- It is possible for you to use a secondary Advanced Threat Defense directly for file submission and report retrieval. However, you are not allowed to modify any of the synchronized configurations.
- Both files and URLs submitted for analysis are distributed to achieve load-balancing.

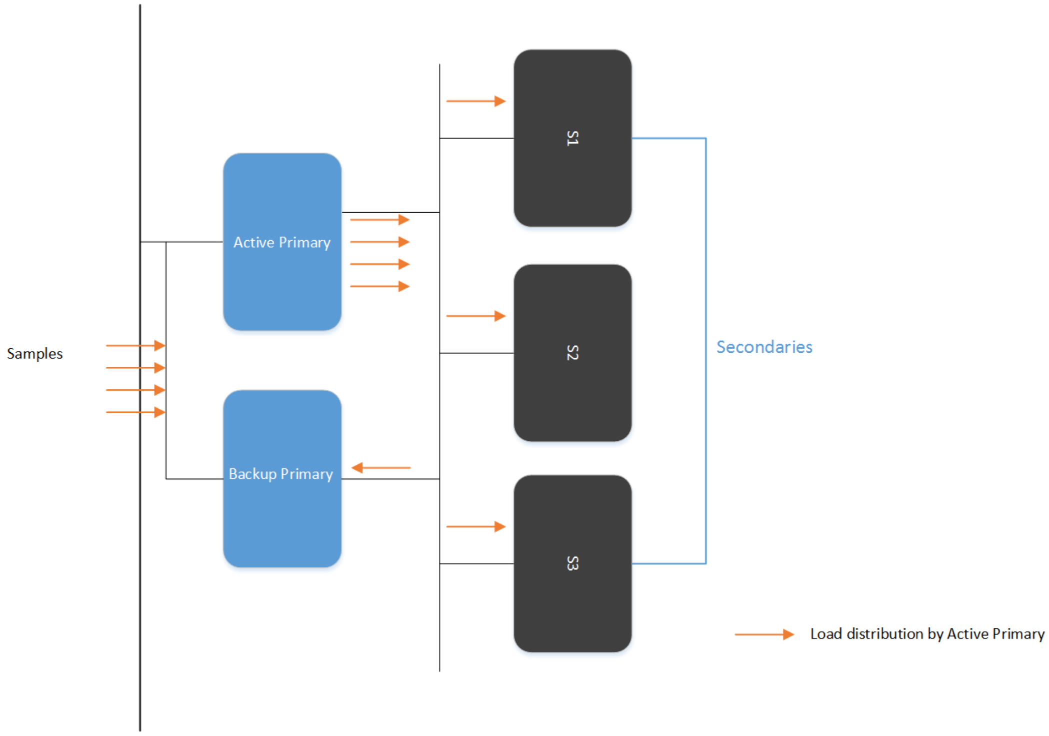


Figure 9-2 Advanced Threat Defense Appliances in a cluster

How are the individual files in a .zip file analyzed by an Advanced Threat Defense cluster?

When you submit a file or URL, Advanced Threat Defense assigns it a unique job ID and a task ID. These IDs are incremental integers. When you submit a .zip file, the component files are extracted and analyzed separately. The job ID for all component files of a .zip file is the same as that of the .zip file's job ID. However, the task ID varies for each component file.

When you submit a .zip file to an Advanced Threat Defense cluster, the primary node identifies the node to which it should distribute the next file and sends the entire .zip file to that node. The node that received the .zip file extracts the component files and analyses them. This applies to .zip files within a .zip file as well.

- If a Sensor submits the .zip file, Advanced Threat Defense generates a cumulative report for the entire .zip file. That is, one report for one .zip file is sent to the Manager when it queries for the report. In case of Web Gateway, .zip files are not supported.
- If you submit a .zip file to the primary node, using its web application for example, individual reports are generated for the component files in the .zip file.

Then the primary node extracts the component files in the zip and distributes them all to the same node for analysis. The primary polls the corresponding secondary for analysis status and results using unique task ID.

How to upgrade the Advanced Threat Defense software for the nodes in a cluster?

Following is the recommended procedure to upgrade the Advanced Threat Defense software for the nodes in a cluster:

1. In a typical load-balancing scenario, first upgrade software of Backup node. The node remains a part of the cluster, however due to version mismatch incoming samples are not submitted to this node. The samples are distributed only between Primary and secondary nodes. The status column of Backup node in the Load-balancing page displays the following message:

   Node is on different software version

2. Upgrade secondary nodes. After you upgrade more than 50 percent of the secondary nodes, upgrade Primary node.

3. Since Primary node remains down during upgrade, Backup node takes over the Active role and distributes the incoming samples between Backup node (Active) and the upgraded secondary nodes. Even after the upgrade of Primary node, Backup node continues to assume the Active role.

4. Upgrade the remaining secondary nodes.

> ! Do not select **Reset Database** when you upgrade any of the nodes. If this option is selected for the primary node, the cluster goes down after upgrade. If the **Reset Database** option is selected for a secondary node, it breaks away from the cluster after upgrade.

Syslog events for Load Balancing

Syslog events are generated for state transition happening for Primary/Backup nodes. These events are generated in 5 minutes time interval, once the state is changed.

Below is a sample output for syslog event generated when state of Primary/Backup node changes from *Active* to *Health Bad* and vice-versa:

```
Dec 13 02:20:01 MATDMIC1U-014 ATD2ESM[771]: {"LB Alert": {"ATD IP": "10.213.248.14",
"Timestamp": "2014-12-13 10:17:39", "Old State": "ACTIVE", "New State": "HEALTH BAD"}
```

```
Dec 13 10:00:02 MATDMIC1U-014 ATD2ESM[23873]: {"LB Alert": {"ATD IP":
"10.213.248.169", "Timestamp": "2014-12-13 17:55:37", "Old State": "HEALTH BAD", "New
State": "ACTIVE"}}
```

Similarily, syslog events are generated for the following scenarios:

- When Primary/Backup node has Load Balancing services status *Down / Up*
- When Load Balancing node state changes from *Active* to *Down* and vice versa
- When there is a configuration mismatch on Backup node from Primary node
- When there is a SW version mismatch on Backup node from Primary node

How to destroy Advanced Threat Defense cluster

Below section deals with procedures to destroy a cluster in following scenarios:

- **Primary is active** - For destroying cluster when primary node is active, administrator logs on to **Load Balancing** page of Advanced Threat Defense to remove/withdraw all other nodes (Backup/ Secondary) one by one. Once all the nodes are removed except primary node, administrator can remove primary node. Removal of primary node is not permitted unless other nodes are removed.

- **Backup is active (Active Primary)** - In this case, as the configured primary is not serving as Active-Primary, the removal of nodes directly from **Load Balancing** page of Advanced Threat Defense is not permitted. Administrator can logon to **Load Balancing** page of Advanced Threat Defense to remove/withdraw all the secondary nodes first, Backup node can then be removed from the cluster. Recall that we cannot have a cluster without a primary node configured, so **Load Balancing** page does not facilitate removal of primary node from cluster. After removing Backup node from cluster if primary node is active, primary node takes the active role (as it does not find the Backup node active). Now, in order to destroy cluster, primary node is removed followed by removal of Backup node.

> If the configured primary is not serving as Active-Primary and Backup is in active state, then the removal of the configured primary requires destroying of cluster.

Methods for removing nodes from cluster:

- **Remove Node from Active-Primary** - This option facilitates removal of secondary/backup node from Active Primary node. If the target node is up at the time of removal, the node changes itself to standalone state and Active Primary removes the entry of the node from the cluster. In case of target node being down at the time of removal, the entry of the target node is removed from the cluster by Active Primary, but once that node comes up, administrator needs to login to the removed node and do a manual cluster withdraw in **Load Balancing** page of Advanced Threat Defense, the role of removed node is then changed to standalone.

- **Withdraw from Cluster at Secondary/Backup Node** - This option is active for all the secondary/backup nodes to withdraw that particular node from Load Balancing.

  > After withdrawal, the entry of the removed node is not deleted from the primary node. Administrator needs to login to primary node and remove that node manually. Please note this node comes to 'Down: Heartbeat not received' state in primary only after Heart Beat (HB) timeout and remains as it is until removed, as it has been withdrawn from the secondary.

- **CLI command: cluster withdraw** - This command is used to destroy cluster using CLI command prompt. It is permitted to run at all nodes (Primary/Backup/Secondary). It wipes out all cluster related configurations from that node and makes it a standalone box. This command can be used in scenarios where normal means of removing a node (Remove Node/Withdraw From Cluster) does not remove that node from cluster. See also cluster withdraw on page 349.

Methods for configuring node to serve as backup:

- **If Backup is not serving as Active Primary** - Administrator deletes the previously configured Backup and adds a new node with backup role.
- **If Backup is serving as Active Primary** - Administrator destroys the cluster and reconfigures Advanced Threat Defense nodes with the new roles.

Process flow for Network Security Platform

Consider a scenario where a Sensor is inline between the endpoints on your network and the Web. This Sensor is integrated with a Advanced Threat Defense cluster consisting of 3 Advanced Threat Defense Appliances.

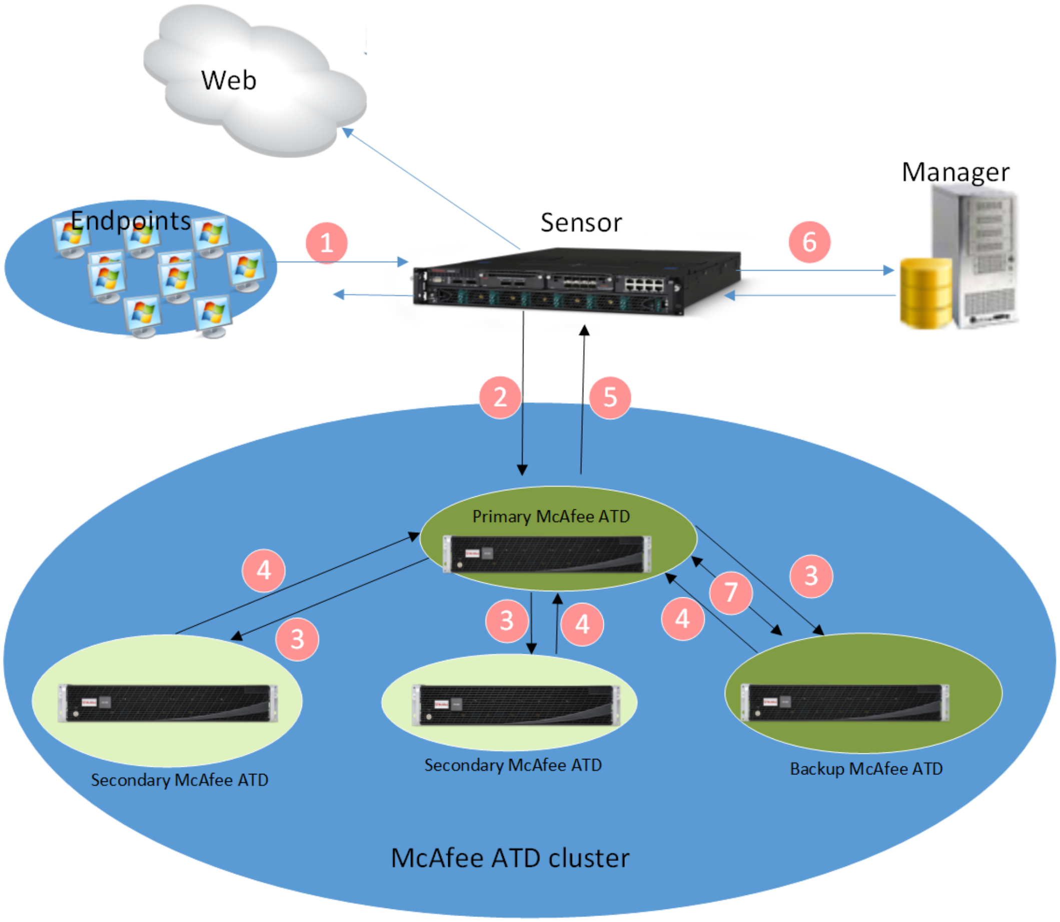


Figure 9-3 Network Security Platform integrated with an Advanced Threat Defense cluster

Number	Description
1	The endpoints attempt to download files from the Web. The inline monitoring ports detect this activity.
2	For a given file, the Sensor withholds the last packet from being forwarded to the endpoint and simultaneously streams the file packets to the primary Advanced Threat Defense for analysis. For this purpose, the Sensor and the primary Advanced Threat Defense use their management ports.
3	After the entire file is with the primary Advanced Threat Defense, it distributes this file to one of the appliances in the cluster. For all communication, the members in the cluster use their management ports.

Number	Description
4	The corresponding secondary Advanced Threat Defense responds with a job ID to the primary and begins to analyze the file based on the user profile. If the file is detected by static analysis, the secondary Advanced Threat Defense sends the malware result (severity) to the primary Advanced Threat Defense.
5	• If the file is detected by static analysis, the primary Advanced Threat Defense sends the malware result that it received from the secondary Advanced Threat Defense to the Sensor's management port. • If the file is dynamically analyzed, the Sensor raises an informational alert in the Real-time Threat Analyzer. This informational alert is set to auto-acknowledge by default, which you can disable if necessary.
6	The Sensor forwards the job ID to the Manager. The Manager queries the primary Advanced Threat Defense Appliance management port for the analysis reports. The primary Advanced Threat Defense pulls the reports from the corresponding Advanced Threat Defense Appliance based on the job ID. Then it forwards the reports to the Manager for display. Also, if the file is found to be malicious based on dynamic analysis, the alert in the Real-time Threat Analyzer is updated accordingly.
7	Backup Advanced Threat Defense assumes Primary Advanced Threat Defense role if Primary Advanced Threat Defense goes down for some reason.

Process flow for McAfee Web Gateway

Consider a scenario where Web Gateway is inline between the endpoints on your network and the Web. This Web Gateway Appliance is integrated with a Advanced Threat Defense cluster consisting of three Advanced Threat Defense Appliances.

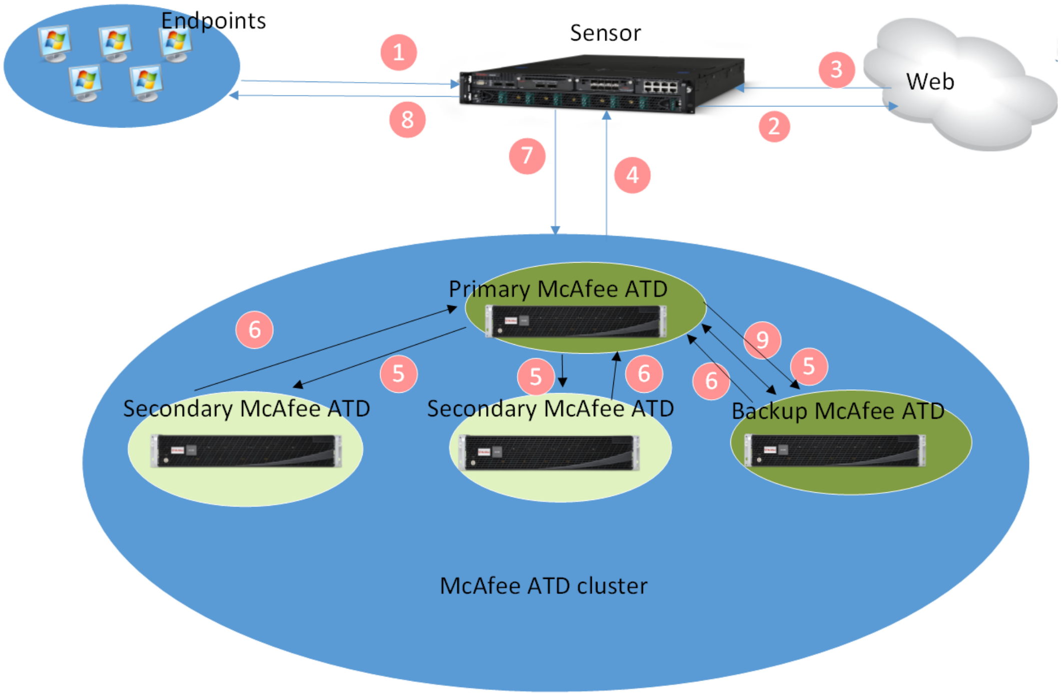


Figure 9-4 Web Gateway integrated with an Advanced Threat Defense cluster

Number	Description
1	The endpoints attempt to download web objects.
2	Web Gateway forwards these requests.

Number	Description
3	When a file is downloaded, the native McAfee Gateway Anti-malware Engine on Web Gateway scans the file and determines the malware score.
4	Based on the file type and the malware score, Web Gateway determines if the file needs to be sent to Advanced Threat Defense for analysis and, if needed, forwards the file to the primary Advanced Threat Defense's management port.
5	The primary Advanced Threat Defense distributes such files among the members based on the number of files submitted to a node. A highly burdened node receives lesser number of samples for processing as opposed to a less burdened node. All communication between the members in a cluster is over their management ports. Assume that the file is sent to one of the secondary Advanced Threat Defense for analysis. The secondary Advanced Threat Defense returns the job ID and task ID to the primary node and begins to analyze the file. The primary node, in turn, returns the job ID and task ID to Web Gateway.
6	For the analysis reports, Web Gateway queries the primary node with the task ID. Using the task ID, the primary node identifies the Advanced Threat Defense that analyzed the file and pulls the reports from it.
7	In response to the query from Web Gateway, the primary Advanced Threat Defense forwards the reports.
8	Based on the report from Advanced Threat Defense, Web Gateway allows or blocks the file accordingly.
9	Backup Advanced Threat Defense assumes Primary Advanced Threat Defense role if Primary Advanced Threat Defense goes down for some reason.

Notes:

- When Web Gateway queries for an MD5 hash value with time period (without the job or task ID), the primary node checks the MD5 hash in its database. If there is no matching record, the primary node checks the secondary nodes where the file is analyzed and sends the report back to Web Gateway without analyzing the corresponding file again.
- When Web Gateway queries for an MD5 hash value for a running task (without the job or task ID), the primary node checks the MD5 hash with status (waiting or analyzing) in its database. If there is no matching record, the primary node checks the secondary nodes where the file is being analyzed or is in the queue. Then the primary node sends the task details back to Web Gateway without analyzing the corresponding file again.

Configuring an Advanced Threat Defense cluster - high-level steps

Follow these high-level steps to configure an Advanced Threat Defense cluster.

1. Identify the Advanced Threat Defense Appliances that you want to use to create the cluster. You can add additional secondary nodes to a working Advanced Threat Defense cluster.
2. Make sure that the Advanced Threat Defense Appliances meet the requirements as discussed in Pre-requisites and considerations on page 320.
3. Identify an unassigned IP address, which is in the same L2 network as are Primary node and Backup node. This IP address is assigned to the cluster.
4. Out of the Advanced Threat Defense Appliances, identify the one that you plan to use as the primary node. All other Advanced Threat Defense Appliances are secondary nodes. Once you define the cluster, you cannot change the primary node without redefining the cluster itself. Similarly, once Backup node is added it cannot be changed unless it is removed from Cluster.

Factor in the following when you decide on the primary node.

- Use the primary node's IP address to submit files and to manage the configuration.
- Products such as Network Security Platform, Web Gateway and Email Gateway must be integrated with the primary node's IP address. Since the result and report retrieval is through the primary, connection between the integrated products and the secondary nodes is not mandatory. With 3.4.2 release, Cluster IP is point of contact for these integrated products, if user chooses to configure a Backup node.
- Make sure the analyzer VMs and VM profiles are identical across all nodes.

  > If you require to add an analyzer VM or if you require to add, modify, or delete a VM profile, break the cluster, make the required changes in all nodes, and then re-create the cluster.

- The synchronized configurations of the secondary are overwritten with that of the primary node. Post cluster creation, you use the primary node to manage these configurations. For information on synchronized configurations, see How the Advanced Threat Defense cluster works? on page 323.

5. Make sure the secondary nodes and the primary node are able to communicate with each other using their management ports.
6. As a best practice, back up the configuration of all nodes, especially the secondary nodes, before you configure the cluster.
7. Make sure that the integrated products are configured to use the primary node. This includes the integrated McAfee products as well as any third-party application or script that use the Advanced Threat Defense REST APIs. With 3.4.2 release Cluster IP is point of contact for these integrated products, if user chooses to configure a backup node.
8. Create the McAfee Advanced Threat Defense cluster on page 331.
9. Submit files and URLs to the Advanced Threat Defense cluster.
10. View the analysis results for an Advanced Threat Defense cluster.
11. Manage configurations for the cluster.

Create the McAfee Advanced Threat Defense cluster

Before you begin

- You have reviewed Configuring an Advanced Threat Defense cluster - high-level steps on page 330.
- You have admin-user rights for the primary node's web application.
- The primary and secondary nodes are not part of any other cluster.
- The software version (active version) of all nodes that you plan to use are an exact match.

Task

1. Identify an Advanced Threat Defense Appliance as the primary node and log on to its web application.

   Use a user name that has admin rights.

2 Select **Manage** | **Load Balancing.**

The **Load Balancing Cluster Setting** page displays.

3 In the **Node IP address** field, enter the management port IP address of the primary node, select **Primary** from the drop - down and click **Add Node.**

4 Confirm if you want to create the cluster.

Advanced Threat Defense sets itself as the primary node for the cluster.

5 In the **Node IP address** field, enter the management port IP address of a secondary node, select **Secondary** and click **Add Node.**

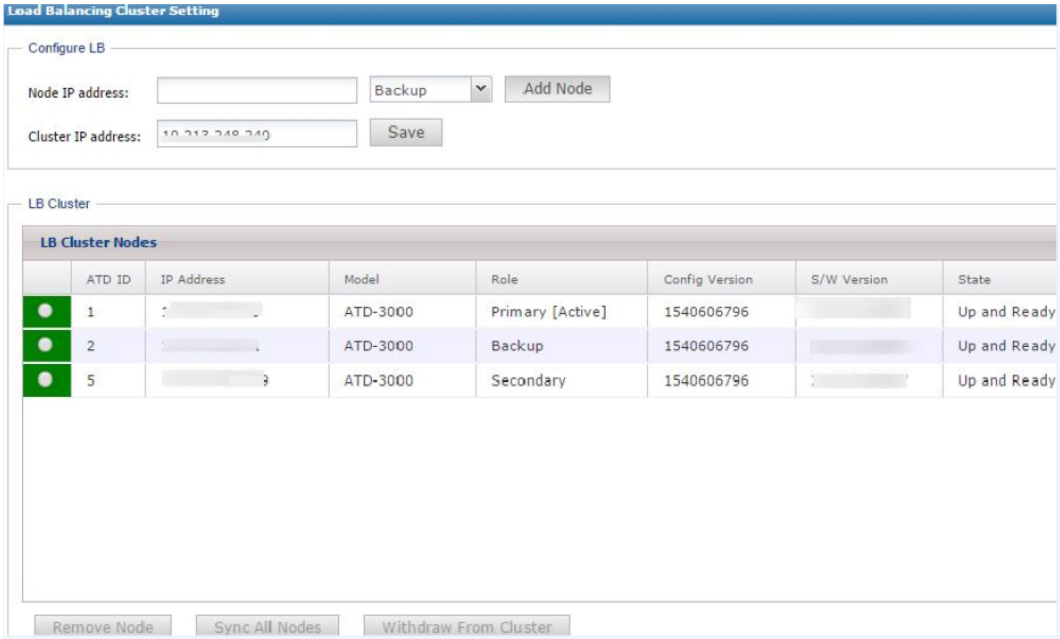
6 Click **Yes** to add the secondary node.

> When you click **Yes** in the confirmation message box, the primary node saves its configuration in a file and sends this to the secondary node. This file contains those configurations, which this document refers to as synchronized configuration. See How the Advanced Threat Defense cluster works? on page 323 for information on synchronized configuration. The secondary uses this configuration file to overwrite the corresponding configuration in its database. So, make sure that you have taken a backup of the secondary's configuration before you proceed. When you remove the secondary from the cluster, it retains the primary node's configuration.

7 Following a similar procedure, add the other secondary nodes.

8 In the **Cluster IP address** field, enter cluster IP address and click **Save**. Select **Backup** from the drop - down and enter the management port IP address of the Backup node in the **Node IP address** field. Click on **Add Node**, Backup node will now be added.

9 The details of all nodes in the cluster are displayed in a table. Similar to other tables in the Advanced Threat Defense web application user-interfaces, you can sort the columns as well as hide or display the required columns.



Load Balancing Cluster Setting

Configure LB

Node IP address: Backup ▾ Add Node

Cluster IP address: 10.213.248.249 Save

LB Cluster

LB Cluster Nodes

	ATD ID	IP Address	Model	Role	Config Version	S/W Version	State
●	1	[redacted]	ATD-3000	Primary [Active]	1540606796	[redacted]	Up and Ready
●	2	[redacted]	ATD-3000	Backup	1540606796	[redacted]	Up and Ready
●	5	[redacted]	ATD-3000	Secondary	1540606796	[redacted]	Up and Ready

Figure 9-5 Advanced Threat Defense cluster creation

> Except for **ATD ID**, **IP Address**, **Role**, and **Withdraw From Cluster**, none of the options are available in the **Load Balancing Cluster Setting** page for the secondary nodes.

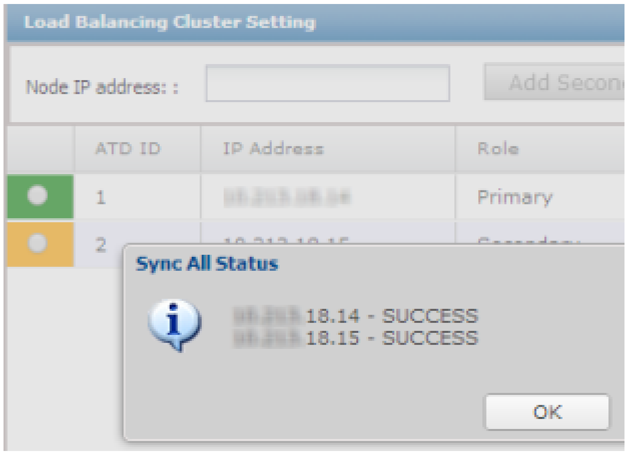
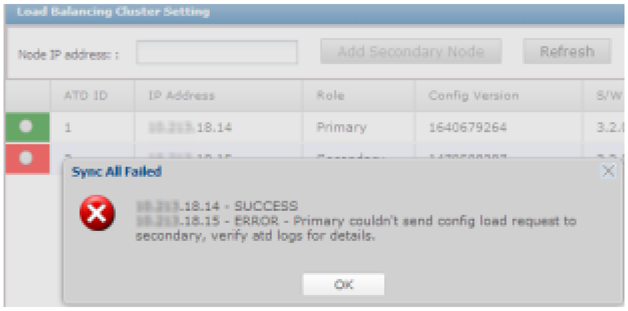
Table 9-1 Option definitions

Option	Definition
Node IP address	Enter the management port IP address of the Advanced Threat Defense Appliance that you want to add to the cluster.
Drop - Down	Select Primary / Backup / Secondary as per the requirement.
Add Node	Click to add the primary, secondary and backup node to the cluster. The primary node or secondary node IP address is the IP address that you use to access the Advanced Threat Defense web application.
Cluster IP address	Enter the cluster IP address to be used by Active node (Primary node or Backup node).
Save	Click to save the cluster IP before adding Backup node.
	Indicates the status of a node. • 🟩: Indicates that the node is up and ready. If it is a secondary, it also means that the primary node is receiving the secondary's heartbeat signal. • 🟧: Indicates that the node is up but needs your attention. For example, the configuration might not be in sync with that of the primary. • 🟥: Indicates that the primary node is receiving the secondary node's heartbeat signal. The primary node distributes files only to those nodes, which are in the green status. If the status of a secondary turns amber or red midway of a file transfer, the primary node allocates the file to the next node in queue.
ATD ID	This is a system-generated integer value to identify the nodes in a cluster. The primary node generates this unique value and assigns it to the nodes in the cluster. This ID is displayed in the Analysis Status and Analysis Results left-hand-side tree structure on the primary node. This enables you to identify the node that analyzed a specific sample. The uniqueness of the ATD ID is based on the IP address of a node as stored in the primary node's database. Consider that you have 3 nodes in the cluster. You remove the secondary node with ATD ID 2 from the cluster and add it back again to the cluster. Then this secondary node is assigned the same ATD ID of 2 if all these conditions are met: • You have not changed the IP address of the node's eth-0 interface (management port). • The primary node's database still has a record for the secondary's IP address.
IP Address	The management port IP address of the node.
Model	The Advanced Threat Defense appliance model type. It could be either ATD - 3000 or ATD - 6000
Role	Indicates if a node is a primary or a secondary or a backup node. It also indicates which node is currently behaving as Active node.

Table 9-1 Option definitions *(continued)*

Option	Definition
Config Version	When you save any of the synchronized configuration, the primary node sends its configuration file to the secondary nodes and also versions this configuration file for reference. For each node, the version number of its latest configuration file is displayed. If the version number of a secondary node does not match with that of the primary, it indicates a possible difference in how the secondary node is configured. So, the status color for that secondary node turns to amber. The reason is also mentioned in the **State** column. Also, the primary node automatically pushes its configuration file to that node. This ensures that all nodes are configured similarly concerning synchronized configuration.
S/W Version	Indicates the Advanced Threat Defense software version of the nodes. The complete software version must exactly match for all nodes. If not, the status turns to amber for the corresponding nodes.
State	Indicates the status of node and any critical information related to that node. Some possible states are: • Up and Ready • Heartbeat not received. • Node is on different config version.
Remove Node	Select a node and click to remove the node from the cluster. The configuration from the primary node is retained even when you remove a secondary node from the cluster. You cannot remove a primary node or a Backup node, if it is in active state, before you remove all secondary nodes. This option is not available for a secondary node.

Table 9-1 Option definitions *(continued)*

Option	Definition
Sync All Nodes	Click **Sync All** to trigger the configuration-synchronization for all secondary nodes in the cluster. When you add a secondary node or when you save any of the synchronized configuration in the primary node, the primary automatically triggers a synchronization to all secondary nodes in green and amber state. Details of the configuration sync are displayed for each node based on the success or failure of the synchronization.  Load Balancing Cluster Setting Node IP address: : Add Secon ATD ID IP Address Role 1 Primary 2 OK Sync All Status [redacted]18.14 - SUCCESS [redacted]18.15 - SUCCESS **Figure 9-6 Configuration sync success**  Load Balancing Cluster Setting Node IP address: : Add Secondary Node Refresh ATD ID IP Address Role Config Version S/W 1 [redacted].18.14 Primary 1640679264 3.2. OK Sync All Failed [redacted].18.14 - SUCCESS [redacted].18.15 - ERROR - Primary couldn't send config load request to secondary, verify atd logs for details. **Figure 9-7 Configuration sync error**
Withdraw from Cluster	This button is relevant only for secondary nodes. Click to withdraw a secondary node from the cluster and to use the secondary node as a standalone Advanced Threat Defense Appliance. Recall that if the primary and Backup nodes are down simultaneously, the load-balancing cluster is down. In the aforementioned case, click **Withdraw from Cluster** in the secondary nodes to withdraw from the cluster and to use the secondary nodes as stand-alone appliances.

Monitor the status of an Advanced Threat Defense cluster

Before you begin

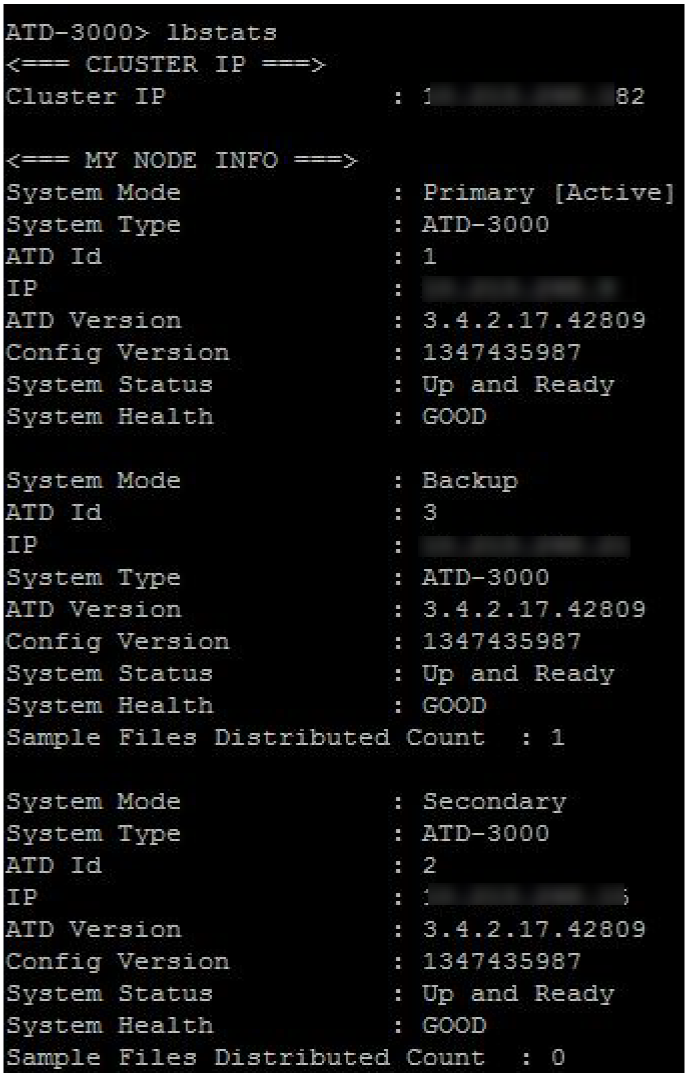
You have successfully created a load-balancing cluster as explained in Create the McAfee Advanced Threat Defense cluster on page 331.

You can monitor the status of an Advanced Threat Defense cluster in the **Load Balancing Cluster Setting** page or by using the `lbstats` command. After configuring cluster IP address, we can login using cluster IP address to access Advanced Threat Defense interface.

Task

1. Log on to the CLI of the primary or a secondary node.
2. Run `lbstats` command.

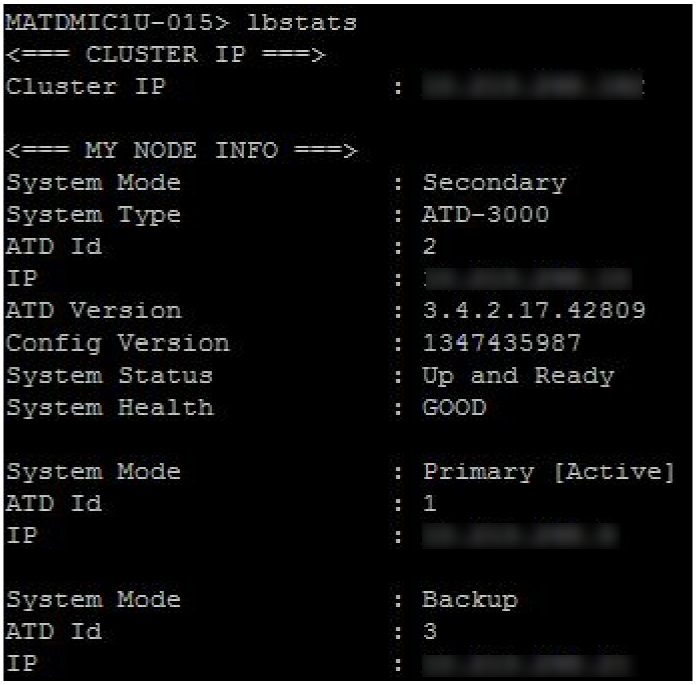
   Separate sections are displayed for each node.



```
ATD-3000> lbstats
<=== CLUSTER IP ===>
Cluster IP                : [redacted]

<=== MY NODE INFO ===>
System Mode               : Primary [Active]
System Type               : ATD-3000
ATD Id                    : 1
IP                        : [redacted]
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD

System Mode               : Backup
ATD Id                    : 3
IP                        : [redacted]
System Type               : ATD-3000
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD
Sample Files Distributed Count  : 1

System Mode               : Secondary
System Type               : ATD-3000
ATD Id                    : 2
IP                        : [redacted]
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD
Sample Files Distributed Count  : 0
```

Figure 9-8 lbstats output from the primary node

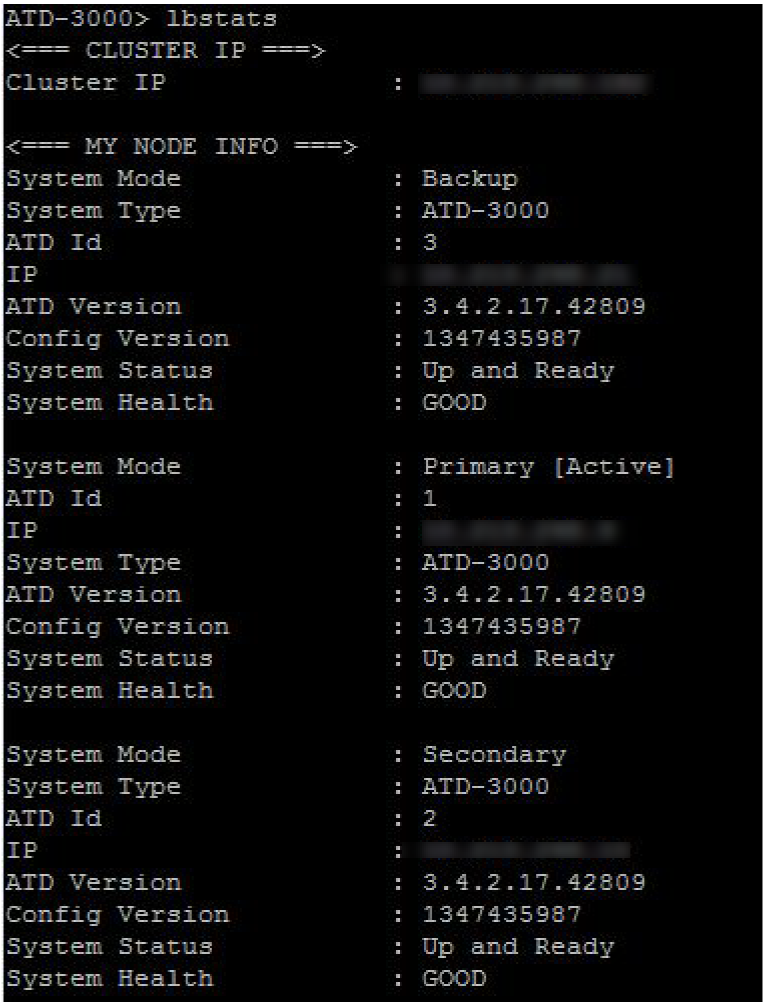
Above is the lbstats output from a primary node.



```
MATDMIC1U-015> lbstats
<=== CLUSTER IP ===>
Cluster IP                : [redacted]

<=== MY NODE INFO ===>
System Mode               : Secondary
System Type               : ATD-3000
ATD Id                    : 2
IP                        : [redacted]
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD

System Mode               : Primary [Active]
ATD Id                    : 1
IP                        : [redacted]

System Mode               : Backup
ATD Id                    : 3
IP                        : [redacted]
```

Figure 9-9 lbstats output from a secondary node

Above is the lbstats output from a secondary node.



```
ATD-3000> lbstats
<=== CLUSTER IP ===>
Cluster IP                    : [redacted]

<=== MY NODE INFO ===>
System Mode                   : Backup
System Type                   : ATD-3000
ATD Id                        : 3
IP                            [redacted]
ATD Version                   : 3.4.2.17.42809
Config Version                : 1347435987
System Status                 : Up and Ready
System Health                 : GOOD

System Mode                   : Primary [Active]
ATD Id                        : 1
IP                            : [redacted]
System Type                   : ATD-3000
ATD Version                   : 3.4.2.17.42809
Config Version                : 1347435987
System Status                 : Up and Ready
System Health                 : GOOD

System Mode                   : Secondary
System Type                   : ATD-3000
ATD Id                        : 2
IP                            : [redacted]
ATD Version                   : 3.4.2.17.42809
Config Version                : 1347435987
System Status                 : Up and Ready
System Health                 : GOOD
```

Figure 9-10 lbstats output from a backup node

Above is the lbstats output from a backup node.

Table 9-2 Details of the lbstats command

Output entry	Description
System Mode	Indicates whether the Advanced Threat Defense Appliance is the primary or a secondary node.
ATD ID	The unique ID assigned to the node.
IP	The management port IP address of the Advanced Threat Defense Appliance.
System Type	The appliance model type. ATD-3000 or ATD-6000.
ATD Version	Advanced Threat Defense software version currently installed on the node.
Config Version	The version of the configuration file currently on the node.
System Status	Whether the node is up and running.

Table 9-2 Details of the lbstats command *(continued)*

Output entry	Description
System Health	Whether the node is in good or an uninitialized state.
Sample Files Distributed Count	The total number of samples distributed among the nodes, including the primary node. This node includes both files and URLs. This data is displayed only when you run `lbstats` on the active node (Primary node or Backup node).

Submitting samples to an Advanced Threat Defense cluster

You use the primary node to submit samples to an Advanced Threat Defense cluster. The process is similar to how you use an individual Advanced Threat Defense Appliance.

- Make sure the integrated products interface with the primary node. When you configure the integration, make sure you use the passwords as configured in the primary node. For example, for Web Gateway, use the *mwg* user name and its password as configured in the primary node. If Backup node is configured then cluster IP address should be the point of contact to for these integrated products.
- To submit files and URLs manually, log on to the primary node with admin rights and submit the files just like how you submit the files to a standalone Advanced Threat Defense Appliance. See Upload files for analysis using Advanced Threat Defense web application on page 284 for step-by-step information.
- You can also use the REST APIs of the primary node to submit files and URLs. See the Advanced Threat Defense APIs Reference Guide for information.
- You can also submit files using FTP or SFTP to the primary node. See Upload files for analysis using SFTP on page 289

> If cluster IP address is configured, we need to login / submit files using cluster ip.

.

Monitor analysis status for an Advanced Threat Defense cluster

The **Analysis Status** page of the primary node displays the analysis status for files analyzed by each node. In a secondary node, only those files analyzed by that secondary node are displayed.

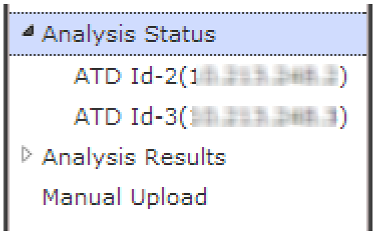
Similar to a standalone Advanced Threat Defense, you can view the status of samples that you submitted. If you have admin rights, you can view the status for samples submitted by any user.

Task

1 Log on to the web application of the primary node.

2 Select **Analysis** | **Analysis Status.**

The **Analysis Status** expands to display the secondary nodes of the cluster. **Analysis Status** corresponds to the primary node. The secondary nodes are listed under **Analysis status** with their ATD ID and their management port IP address.



3 To view the status of the files analyzed by the primary node, click **Analysis Status**.

4 To view the status of files analyzed by a specific secondary node, click the corresponding ATD ID.

For the details of the options in the **Analysis Status** page, see Configure the Analysis Status page on page 293.

Monitor analysis results for an Advanced Threat Defense cluster

The **Analysis Results** page of the primary node displays the analysis results for files analyzed by each node. In a secondary node, only those files analyzed by that secondary node are displayed.

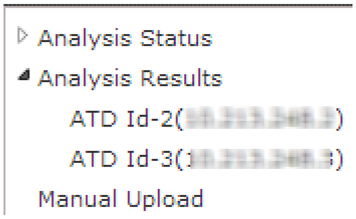
Similar to a standalone Advanced Threat Defense, you can view the results of samples that you submitted. If you have admin rights, you can view the results for samples submitted by any user.

Task

1 Log on as the *admin* user in one of the nodes of the Advanced Threat Defense cluster.

2 Select **Analysis** | **Analysis Results.**

The **Analysis Results** expands to display the secondary nodes of the cluster. **Analysis Results** corresponds to the primary node. The secondary nodes are listed under **Analysis Results** with their ATD ID and their management port IP address.



▷ Analysis Status

◢ Analysis Results

ATD Id-2([redacted])

ATD Id-3([redacted])

Manual Upload

3 To view the results of the files analyzed by the primary node, click **Analysis Results**.

4 To view the results of files analyzed by a specific secondary node, click the corresponding ATD ID.

For the details of the options in the **Analysis Results** page, see View the analysis results on page 295.

Modifying configurations for a Advanced Threat Defense cluster

Regarding an Advanced Threat Defense cluster, configurations can be classified into two types:

- Settings that you configure only from the primary node. For the sake of explanation, these settings are referred as *synchronized configuration* in this document.
- Settings that you configure individually in each node of a Advanced Threat Defense cluster. These settings are referred as *unsynchronized configuration*.

Synchronized configuration — The following are the settings that fall under this category:

- Managing analyzer profiles on page 239
- Managing McAfee Advanced Threat Defense users on page 37
- Integration with McAfee ePO for OS profiling on page 243
- Configure proxy servers for Internet connectivity on page 254
- Configure DNS setting on page 261
- Configure date and time settings on page 262

Log on to the primary node with admin rights to configure these settings listed above. When you click **Save** in the corresponding pages, the primary node bundles the entire *synchronized configuration* in a file and sends it to all available secondary nodes. The secondary nodes save these settings in their database and use these settings later. This configuration file is assigned a version number. This version number is the **Config Version** listed in the **Load Balancing Cluster Setting** page.

The primary node sends the configuration file over a secure communication channel to the secondary nodes. You can verify the **State** column in the **Load Balancing Cluster Setting** page to verify if the configuration file was successfully applied on a secondary node. Alternatively, you can click **Sync All Nodes** in the **Load Balancing Cluster Setting** page for the primary node to send the configuration file to all available nodes. If a secondary node is down, it is indicated in the **State** column.

> When the primary node synchronizes configuration for the cluster, it sends the complete *synchronized data* to all available nodes in the cluster. That is, you cannot selectively synchronize secondary nodes. Neither can you select the configurations that you want sent to the secondary nodes. However, the configuration-synchronization process does not affect the load-balancing or file-analysis processes of a Advanced Threat Defense Appliance.

Unsynchronized configuration — The following are the settings that fall under this category:

- McAfee Advanced Threat Defense software version.
- Creating analyzer VM on page 4
- Managing VM profiles on page 222
- DAT and engine versions of McAfee Anti-Malware Engine.
- DAT and engine versions of McAfee Gateway Anti-Malware Engine.
- Whitelist and blacklist entries.
- Custom YARA rules
- Database backup and restore configurations.
- Any configuration done using the CLI.

Log on to each node in the cluster to change these configurations. Make sure that these configurations are same in all nodes of the cluster.

10 CLI commands for McAfee Advanced Threat Defense

The McAfee Advanced Threat Defense Appliance supports command-line interface (CLI) commands for tasks such as network configuration, restarting the Appliance, and resetting the Appliance to factory defaults.

Contents

Issue of CLI commands

You can issue CLI commands locally, from the McAfee Advanced Threat Defense Appliance console, or remotely through SSH.

How to issue a command through the console

For information on how to set up the console for a McAfee Advanced Threat Defense Appliance, see Configure network information for Advanced Threat Defense Appliance on page 31.

> When the documentation indicates that you must perform an operation "on the Appliance," it signifies that you must perform the operation from the command line of a console host connecting to the McAfee Advanced Threat Defense Appliance. For example, when you first configure the network details for a McAfee Advanced Threat Defense Appliance, you must do so from the console.

When you are successfully connected to the McAfee Advanced Threat Defense Appliance, you will see the login prompt.

Issuing a command through SSH

You can administer a McAfee Advanced Threat Defense Appliance remotely from a command prompt over `ssh`.

Logging on to the McAfee Advanced Threat Defense Appliance using an SSH client

Task

1. Open an SSH client session.
2. Enter the IPv4 address of the McAfee Advanced Threat Defense Appliance and enter 2222 as the SSH port number.
3. At the logon prompt, enter the default user name `cliadmin` and password `atdadmin`.

   The number of logon attempts to the McAfee Advanced Threat Defense Appliance from a client, on a single connection, is set to 3, after which the connection is closed.

   > The number of logon attempts to the McAfee Advanced Threat Defense Appliance can differ based on the ssh client that you are using. You can get three logon attempts with certain clients (for example, Putty release 0.54, Putty release 0.56) or you can get four logon attempts with other clients (for example, Putty release 0.58, Linux ssh clients).

Auto-complete

The CLI provides an auto-complete feature. To auto-complete a command, press **Tab** after typing a few characters of a valid command and then press **Enter**. For example, typing `pas` and pressing **Tab** would result in the CLI auto-completing the entry with the command `passwd`.

If the partially entered text matches multiple options, the CLI displays all available matching commands.

CLI syntax

You issue commands at the command prompt as shown.

```
<command> <value>
```

- Values that you must enter are enclosed in angle brackets (< >).
- Optional keywords or values are enclosed in square brackets ([ ]).
- Options are shown separated by a line (|).
- Variables are indicated by *italics*.

> Do not type the < or [ ] symbols.

Mandatory commands

There are certain commands that must be executed on the McAfee Advanced Threat Defense Appliance before it is fully operational. The remaining commands in this chapter are optional and will assume default values for their parameters unless they are executed with other specific parameter values.

These are the required commands:

- `set appliance name`
- `set appliance ip`

- `set appliance gateway` is also required if any of the following are true:
  - If the McAfee Advanced Threat Defense Appliance is on a different network than the McAfee products you plan to integrate
  - If you plan to access McAfee Advanced Threat Defense from a different network either using an SSH client or a browser for accessing the McAfee Advanced Threat Defense Web Application

Log on to the CLI

Before you can enter CLI commands, you must first log on to the McAfee Advanced Threat Defense Appliance with a valid user name (default user name is `cliadmin`) and password (default is `atdadmin`). To log off, type `exit`.

McAfee strongly recommends you change this password using the `passwd` command within your first interaction with the McAfee Advanced Threat Defense Appliance.

Meaning of "?"

`?` displays the possible command strings that you can enter.

Syntax

```
?
```

If you use `?` in conjunction with another command, it shows the next word you can type. If you execute the ? command in conjunction with the `set` command, for example, a list of all options available with the `set` command is displayed.

Managing the disks of McAfee Advanced Threat Defense Appliance

The McAfee Advanced Threat Defense Appliance has two disks referred to as disk-A and disk-B. Disk-A is the active disk and disk-B is the backup disk. Even if disk-A is not booted, it is referred as the active disk. Similarly, even if disk-B is the booted disk, it is referred as the backup disk. By default, both these disks contain the pre-installed software version.

Use the `show` command to view the software version stored in the active and backup disks.

Table 10-1 CLI commands for managing the disks

Command	Description
`copyto backup`	Copies the software version on the active disk to the backup disk. For example, if you find the current active software version to be stable, you can back it up to the backup disk. This command works only if the Appliance had been booted from the active disk.
`copyto active`	Copies the software version from the backup disk to the active disk. However, you must restart the McAfee Advanced Threat Defense Appliance for it to load this new image from the active disk. This command works only if the Appliance had been booted from the backup disk.
`reboot backup`	Reboots the Appliance with the software version on the backup disk.
`reboot active`	Reboots the Appliance with the software version on the active disk.

List of CLI commands

This section lists McAfee Advanced Threat Defense CLI commands in the alphabetical order.

amas

Use this command to restart/start/stop the amas services.

Syntax: `amas <word>`

Parameter	Description
<WORD>	The amas service you want to stop.

Example: `amas start/stop/restart`

atdcounter

Dsiplays the engine specific counter e.g. files sent and processed by GTI, MAV, GAM, Amas and so on.

Syntax: `atdcounter`

This command has no parameters.

backup reports

Use this command to create a backup of the McAfee Advanced Threat Defense reports on an external FTP/SFTP server configured for a user under the FTP results output setting interface ports.

Syntax

```
backup reports
```

This command has no parameters.

backup reports date

This command creates a backup of the McAfee Advanced Threat Defense reports for a particular date range on an external FTP/SFTP server configured for a user under the FTP results output setting.

Syntax: `backup reports date <yyyy-mm-dd>`

Parameter	Description
yyyy-mm-dd yyyy-mm-dd	The date range for which you want to create a backup for reports.

Example: `2014-07-10 2014-07-12`

Blacklist

Use the following commands to manage the blacklist of McAfee Advanced Threat Defense.

Syntax:

- To add an MD5 to the blacklist, use `blacklist add <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to add to the blacklist.
<score>	The malware severity score. A valid value is from 3 to 5.
<file_name>	The file name for the MD5.
<malware_name>	The malware name for the MD5.
<Eng-ID>	The numerical ID for the engine that detected the malware. Following is the numerical coding. Sandbox — 0, GTI — 1, GAM — 2, Anti-Malware — 4.
<OS-ID>	The numerical ID of the operating system that was used to dynamically analyze the malware.

  Example: `blacklist add 254A40A56A6E28636E1465AF7C42B71F 3 ExampleFileName ExampleMalwareName 4 2`

- To delete an MD5 from the blacklist, use `blacklist delete <md5>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to delete from the blacklist.

  Example: `blacklist delete 254A40A56A6E28636E1465AF7C42B71F`

- To check if an MD5 is present in the blacklist, use `blacklist query <md5>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to query if it is present in the blacklist.

  Example: `blacklist query 254A40A56A6E28636E1465AF7C42B71F`

  If the MD5 is present, the details such as the engine ID, malware severity score, and so on, are displayed.

- To update the details for an entry in the blacklist, use `blacklist update <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to update. This value must exist in the blacklist for you to update the record.
<score>	The new malware severity score that you want to change to. A valid value is from 3 to 5.
<file_name>	The new file name for the MD5.
<malware_name>	The new malware name for the MD5.
<Eng-ID>	The new engine ID that you want to change to.
<OS-ID>	The new value for the operating system that was used to dynamically analyze the malware.

Example: `blacklist update 254A40A56A6E28636E1465AF7C42B71F 4 ExampleFileName ExampleMalwareName 2 4`

clearstats all

Use this command to reset all the McAfee Advanced Threat Defense statistics to zero.

Syntax: `clearstats all`

This command has no parameters.

The following information is displayed using this command:

```
<=== DXL STATUS ===>
Status                                      : DISABLED
DXL Channel Status                          : DOWN
Sample Files Received Count                 : 0
Sample Files Published Count                : 0
Sample Files Queued Count                   : 0
```

clearstats dxl

Use this command to reset the DXL file counter to zero.

Syntax: `clearstats dxl`

This command has no parameters.

The following information is displayed using this command.

```
All DXL stats are reset to zero
Sample Files Received Count                 : 0
Sample Files Published Count                : 0
```

clearstats lb

Use this command to reset all the McAfee Advanced Threat Defense load-balancing statistics to zero.

Syntax: `clearstats lb`

This command has no parameters.

The following information is displayed using this command:

```
LB stats are reset to zero
```

clearstats tepublisher

Use this command to clear the count of events sent to ePO.

Syntax: `clearstats tepublisher`

This command has no parameters.

The following information is displayed using this command:

```
All TEP stats are reset to zero
Sample Files Received Count              : 0
Sample Files Published Count             : 0
```

cluster withdraw

This command is used to destroy cluster using CLI command prompt. It is permitted to run at all nodes (Primary/Backup/Secondary). It wipes out all cluster related configurations from that node and makes it as a standalone box.

This command can be used in scenarios where normal means of removing a node (Remove Node/ Withdraw From Cluster) does not remove that node from cluster.

Syntax: `cluster withdraw`

This command has no parameters.

createDefaultVms

Use this command to create default analyzer VMs.

Syntax: `createDefaultVms`

This command has no parameters.

db_repair

Repairs the ATD database in case the database gets corrupt.

Syntax: `db_repair`

This command has no parameters.

deleteblacklist

Use this command to remove all the entries from McAfee Advanced Threat Defense blacklist.

Syntax: `deleteblacklist`

This command has no parameters.

deletesamplereport

Deletes all the analysis reports for a file.

Syntax: `deletesamplereport <md5>`

Parameter	Description
<md5>	The MD5 value of the file for which you want to delete all the reports in McAfee Advanced Threat Defense.

Example: `deletesamplereport c0850299723819570b793f6e81ce0495`

diskcleanup

Use this command to delete some of the older analysis reports if the disk space of McAfee Advanced Threat Defense is low.

Syntax: `diskcleanup`

This command has no parameters.

dxlstatus

Use this command to know the status of DXL.

Syntax: `dxlstatus`

This command has no parameter.

The following information is displayed using this command:

```
<=== DXL STATUS ===>
Status                                      : DISABLED
DXL Channel Status                          : DOWN
Sample Files Received Count                 : 0
Sample Files Published Count                : 0
Sample Files Queued Count                   : 0
```

docfilterstatus

Docfilterstatus command helps in higher performance of Advanced Threat Defense Appliance by bypassing the dynamic analysis of MS Office 2007+ Power Point files (pptx) that have no suspicious embedded content or malicious hyperlinks. Only suspicious pptx files are analyzed in sandbox and clean pptx files are spared from entering the sandbox.

The docfilterstatus command is introduced to avoid unnecessary sandbox loading by MS Office 2007+ Word and Excel files when they contain no suspicious content. The command allows enabling or disabling of the heuristic filter for MS Office 2007+ Word and Excel files.

By default, docfilterstatus is enabled.

Syntax:

```
set docfilterstatus <enable>
```

```
set docfilterstatus <disable>
```

Parameter	Description
enable	Sets the sample filtering to "on" or enables docfilterstatus operation
disable	Sets the sample filtering to "off"or disables docfilterstatus operation

When docfilterstatus is enabled:

- Docfilterstatus filtering is ON.

  Enabling docfilterstatus sets docfilterstatus to ON. Advanced Threat Defense Appliance scans MS Office 2007+ Word or Excel files structure for any abnormalities. If there are no abnormalities, the file is treated as a clean and there is no further analysis. If there are any heuristic abnormalities, the MS Office 2007+ Word or Excel file is statically and dynamically analyzed as per the corresponding analyzer profile.

When docfilterstatus is disabled:

- Docfilterstatus is OFF.

  Disabling docfilterstatus sets docfilterstatus to OFF. Advanced Threat Defense Appliance does not scan MS Office 2007+ Word and Excel files for any heuristic abnormalities. MS Office 2007+ Word and Excel files are statically and dynamically analyzed as per the corresponding analyzer profile.

Use the show command to know the current filter setting.

Syntax: `show docfilterstatus`

Exit

Exits the CLI.

This command has no parameters.

Syntax:

```
exit
```

factorydefaults

Deletes all samples, results, logs, and analyzer VM images, and it resets IP addresses before rebooting the device. This command does not appear when you type `?` nor does the auto-complete function applies to this command. You must type the command in full to execute it.

This command has no parameters.

- You are warned that the operation will clear McAfee Advanced Threat Defense Appliance and you must confirm the action. The warning occurs since the McAfee Advanced Threat Defense Appliance returns to its clean, pre-configured state, thus losing all current configuration settings in both the active and backup disks. Once you confirm, this command immediately clears all your configuration settings, including samples, results, logs, and analyzer VM images, in both the active and backup disks.
- The current software version in the backup disk is applied on the active disk.

Syntax:

```
factorydefaults
```

filetypefilter

Use this command, if you want Advanced Threat Defense to consider the file based on the extension the file carries and not only by the file header before sending it for dynamic analysis.

Syntax:`filetypefilter<enable><disable><status>`

Parameter	Description
status	Displays whether the *filetypefilter* feature is enabled or disabled currently. By default, it is disabled.
enable	Sets the sample filtering on. When it is enabled, Advanced Threat Defense considers following supported file types for analysis. *.7z, .ace, .apk, .arj, .bat, .cab, .cgi, .chm, .class, .cmd, .com,* *.dll, .doc, .docm, .docx, .dotm, .dotx, .eml, .exe, .htm,* *.html, .inf, .ins,. js, .lnk, .lzh, l.zma, .mof, .msg,* *.ocx, .pdf, .potm, .potx, .ppam, .pps, .ppsm, .ppsx*
disable	Sets the sample filtering to off. When it is disabled, McAfee Advanced Threat Defense considers only the file types supported by default for dynamic analysis.

ftptest USER_NAME

Use this command to test the FTP settings saved under MANAGE > USER MANAGEMENT > FTP Results (for a particular user).

Syntax: `ftptest USER_NAME`

Parameter	Description
USER_NAME	The user name for which you want to test the FTP settings

Example: `NSPuser`

gti-restart

Restarts the McAfee GTI engine of McAfee Advanced Threat Defense.

Syntax: `gti-restart`

This command has no parameters.

help

Provides a description of the interactive help system.

This command has no parameters.

Syntax:

```
help
```

heuristic_analysis

Consider a scenario where there is a very high volume of files submitted by a channel like Network Security Sensor, Web Gateway, or Email Gateway. You want Advanced Threat Defense to triage these files based on a need for detailed malware analysis. The intention of this triage is to scale up performance without compromising on security. The heuristic_analysis command is introduced to meet such a requirement.

- Enable the heuristic filter for PDF files.
- Disable the re-analyze option for all supported file types.

Use the `show` command to know the current status. By default, heuristic analysis is disabled.

Syntax: `show heuristic_analysis`

When heuristic analysis is disabled, the following are the settings:

Setting	Description
`Heuristic filtering is OFF`	This is a feature of Advanced Threat Defense. When turned on, Advanced Threat Defense does a heuristic analysis of a PDF file, MS Office 2007+ Word, and MS Office 2007+ Excel file submitted by a channel like Network Security Sensor, Web Gateway, or Email Gateway. That is, it examines the structure of the files for any malicious content such as embedded Java scripts, embedded .exe files, or any redirections. Only if there are heuristic abnormalities in the file, it is considered for malware analysis as per the corresponding analyzer profile. If there are no abnormalities, the file is treated as clean. That is, a severity rating of zero (information) is assigned. In networks where there is a very high flow of PDF files, the heuristic filter can reduce the load on Advanced Threat Defense by filtering off files that do not have any suspicious content.
`configuration setting: re-analysis: ON`	By default, Advanced Threat Defense analyses all the supported files submitted by a Sensor even if the files have already been analyzed. When re-analysis is set to OFF, Advanced Threat Defense checks if analysis results are already available for a file based on its MD5 hash value. If yes, then it provides the available result to Network Security Manager instead of re-analyzing the file. The same result is displayed in Advanced Threat Defense as well.

The re-analysis function applies to all supported file types supported by Sensors, whereas the heuristic filter apply only to PDF files submitted by Sensors. `set heuristic_analysis` command displays `configuration setting: re-analysis: OFF` message. This message is applicable only if the Advanced Threat Defense is integrated with Network Security Platform devices. If you integrate Advanced Threat Defense with non-NSP device(s), you can safely ignore this message.

Use the `set` command to enable or disable heuristic analysis for files submitted by a Sensor.

Syntax: `set heuristic_analysis <enable>`

Syntax `set heuristic_analysis <disable>`

http_redirect

The `http_redirect` command can be used to enable or disable redirecting of *http* request to *https* on browser. Secure access to Advanced Threat Defense Appliance is ignored when `http_redirect` is disabled.

Syntax:

```
set http_redirect
```

The http to *https* redirection can either be enabled or disabled using this command. Any sample submitted during the command execution is rejected as *lighttpd* is restarted.

Parameter	Description
enable	When `http_redirect` feature is enabled, *http* url is redirected to *https* on browser. RestAPI calls with only *https* protocol are accepted.
disable	When `http_redirect` feature is disabled, *http* when requested on browser is not redirected to *https*. RestAPI calls with either *http* or *https* protocol are accepted.

It is advised to have this feature enabled all the time. You must disable this feature in case of issues with certificate validation.

Use the `show http_redirect` to know whether the *http* to *https* redirect feature is currently enabled or disabled on the Advanced Threat Defense Appliance device. By default, the redirect feature is enabled.

Syntax: `show http_redirect`

install msu

Installs either of the two below listed msu files:

- *amas-3.x.x.x.x.msu*
- *system-3.x.x.x.x.msu*

Syntax:

```
install msu
```

Parameter	Description
`<SWNAME>`	msu filename that user wants to install. Either amas-3.x.x.x.x.msu or system-3.x.x.x.x.msu.
`<RESET_DB>`	This parameter accepts two values (0/1). '0' indicates msu file to be installed without resetting the database. '1' indicates msu file to be installed alongwith resetting the database.

Example: `install msu amas-3.3.0.25.42303.msu 1`

lbstats

Shows the statistics for Primary node, Back up node and Secondary node in a load-balancing cluster.

This command has no parameters. No output is displayed if the Advanced Threat Defense is not part of a cluster.

Syntax:

```
lbstats
```

For the details see, Monitor the status of an Advanced Threat Defense cluster on page 335.

list

Lists all the CLI commands available to users.

Syntax: `list`

This command has no parameters.

lowseveritystatus

Advanced Threat Defense treats severity 1 and 2 samples as low-severity and severity 3, 4, and 5 as malicious. By default, if you configure dynamic analysis, the dynamic analysis score is displayed in the summary report for all samples. This score also affects the final score for that sample. If necessary, you can use the `lowseveritystatus` command to alter this behavior. For example, for low-severity samples that are dynamically analyzed, Advanced Threat Defense does not display the dynamic analysis score in the summary report nor consider this score for computing the final score.

The `lowseveritystatus` command applies only to non-PE samples such as Microsoft Word documents and PDF files.

Syntax: `lowseveritystatus <show><hide>`

Example: `lowseveritystatus hide`

Parameter	Description
`show`	This is the default behavior. If a sample is dynamically analyzed, Advanced Threat Defense displays the dynamic analysis score in the report. It also considers this score to compute the final score.
`hide`	Assume that the sample is a non-PE file, which has undergone dynamic analysis. If Advanced Threat Defense detects the file to be low-severity, it does not display the dynamic analysis score in the report (under **Sandbox** in the **Down Selector's Analysis** section). Advanced Threat Defense also does not consider the dynamic analysis score for computing the final score. However, the details of the dynamic analysis such as files opened and files created are included in the report. The `lowseveritystatus hide` command affects only the score displayed in the report and does not affect how the results are displayed in the **Analysis Results** page.

nslookup

Displays nslookup query result for a given domain name. You can use this to verify if McAfee Advanced Threat Defense is able to perform nslookup queries correctly.

Syntax: `nslookup <WORD>`

Parameter	Description
<WORD>	The domain name for which you want to query for nslookup.

Example: `nslookup mcafee.com`

passwd

Changes the password of the CLI user (cliadmin). A password must be between 8 and 25 characters in length and can consist of any alphanumeric character or symbol.

You are asked to enter the current password before changing to a new password.

Syntax:

```
passwd
```

ping

Pings a network host or domain name. You can specify an IPv4 address to ping network host and domain name if you wish to ping domain name.

Syntax:

```
ping <A.B.C.D>
```

Parameter	Description
<A.B.C.D>	Denotes the 32-bit network host IP address written as four eight-bit numbers separated by periods. Each number (A, B, C or D) is an eight-bit number between 0–255.
<WORD>	The domain name you want to ping.

quit

Exits the CLI.

This command has no parameters.

Syntax:

```
quit
```

reboot

Reboots the McAfee Advanced Threat Defense Appliance with the image in the current disk. You must confirm that you want to reboot.

Syntax:

```
reboot
```

Parameter	Description
`reboot active`	Reboots the Appliance with the software version on the active disk.
`reboot backup`	Reboots the Appliance with the software version on the backup disk.
`reboot vmcreator`	Recreates the analyzer VMs configured in the McAfee Advanced Threat Defense web application, while rebooting the Appliance.

remove

This command removes all original samples from ATD for which analysis is complete.

The remove command has these parameters:

- `now`: When executed, immediately removes the *original samples* for all the completed samples present on ATD. Even if you enable **Sample Download Access**, you cannot download the sample.
- `enable`: When executed, immediately removes the *original samples* for all the completed samples present on ATD. It also enables you to set a daily task to automatically remove *original samples* from newly completed samples at a configured time.
- `disable`: When executed, disables the daily task to remove *original samples* from newly completed sample files at the configured time.

Syntax: `remove samples all <now><enable><disable>`

Example 1: `ATD-6000> remove samples all now`

```
Removing all sample files now...

10 sample files removed
```

Example 2: `ATD-6000> remove samples all enable 11:37:14`

```
Removing all sample files now...
```

```
14 sample files removed
```

```
Setting up daily task to remove newly completed sample files at 11:37:14
```

Example 3: `ATD-6000> remove samples all disable`

```
Disabling daily task
```

removenetworkaddress

This command removes IP, subnet mask and gateway address from Advanced Threat Defense Appliance. The changes are reflected after the box is rebooted. This is a hidden command, useful for support personnel.

Syntax: `removenetworkaddress`

This command has no parameters.

Example: `ATD-6000> removenetworkaddress`

```
Remove the appliance network addresses ?
```

```
Please enter Y to confirm:
```

removeSampleInWaiting

Use this command to remove all the sample waiting to be analyzed by McAfee Advanced Threat Defense.

Syntax: `removeSampleInWaiting`

This command has no parameters.

The following information is displayed using this command:

```
Starting the sample queue cleaning...
The cleaning is done
```

resetuiadminpasswd

Use this command to reset the password for the *admin* user of McAfee Advanced Threat Defense web application. When you execute this command, the password is reset to the default value, which is *admin*. Note that the currently logged on sessions are not affected. A change in password affects only new logon attempts.

Syntax: `resetuiadminpasswd`

Press Y to confirm or N to cancel.

resetusertimeout

Enables users to log on to McAfee Advanced Threat Defense web application without waiting for the timer to expire.

Syntax: `resetusertimeout <WORD>`

Parameter	Description
<WORD>	The McAfee Advanced Threat Defense web application user name for which you want to remove the logon timer. If this action is successful, the message *Reset done!* is displayed.

Example: `resetusertimeout admin`

restart network

Use this command to restart network on the McAfee Advanced Threat Defense. Restart amas after using this command.

Syntax: `restart network`

This command has no parameters.

revertwebcertificate

Use this command to revert back uploaded web certificate to the default certificate.

Syntax: `revertwebcertificate`

This command has no parameters.

The following information is displayed using this command:

```
revertwebcertificate
Successfully reverted back web certificate to default!
Restarting lighttpd service!
```

route add/delete network

CLI commands are available for adding and deleting static route to McAfee Advanced Threat Defense.

To add a port

```
route add network <network ip> netmask <netmask> gateway <gateway ip> intfport <port
number 1><port number 2><port number 3>
```

Example: `route add network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

To delete a port

```
route delete network <network ip> netmask <netmask> gateway <gateway ip> intfport
<port number 1><port number 2><port number 3>
```

Example: `route delete network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

samplefilter

This command is specific to Network Security Platform Sensors. Use this command to prevent Sensors from sending unsupported file types to McAfee Advanced Threat Defense for analysis.

Syntax:

```
samplefilter <status><enable><disable>
```

Parameter	Description
status	displays whether the sample filtering feature is enabled or disabled currently. By default, it is enabled.
enable	sets the sample filtering on. When it is enabled, McAfee Advanced Threat Defense considers only the supported file types from Network Security Platform for analysis. Refer to Analyzing malware on page 5 for the list of supported files. McAfee Advanced Threat Defense ignores all other file types and also informs Network Security Platform that a sample is of an unsupported file type . This prevents resources being spent on unsupported file types on both McAfee Advanced Threat Defense and Network Security Platform.
disable	sets the sample filtering to off. When disabled, McAfee Advanced Threat Defense considers all the files submitted by Network Security Platform for analysis but only the supported file types are analyzed. The remaining are reported as unsupported in the **Analysis Status** and **Analysis Results** pages.

Example:

```
samplefilter status
```

set appliance dns A.B.C.D E.F.G.H WORD

Sets Advanced Threat Defense Appliance preferred and alternate DNS address.

Syntax:

```
set appliance dns A.B.C.D E.F.G.H WORD
```

Parameter	Description
`<A.B.C.D>`	DNS preferred address
`<E.F.G.H>`	DNS alternate address
`<WORD>`	Appliance domain name

Example: `ATD-6000> set appliance dns 1.1.1.2 10.11.10.4 nai.com`

```
DNS setting had been configured
```

set gti dns check

This command requires DNS to be set for GTI to work. By default this command is set to disabled, which means that if there is no internet access, GTI works fine. If this command is enabled, GTI will not work unless ATD is connected to the Internet and resolves GTI lookup URLs. You need to restart amas for these changes to reflect on ATD.

Syntax: `set gti dns check <enable><disable>`

Example: `ATD-6000> set gti dns check enable`

```
DNS access check is now enabled

ATD-6000> set gti dns check disable

DNS access check is now disabled
```

set intfport

Use this command to enable or disable McAfee Advanced Threat Defense interface ports.

Syntax

```
set intfport <1><2><3> <enable><disable>
```

Example: `set intfport 1 enable`

set intfport auto

Sets an interface port to auto-negotiate the connection with the immediate network device.

Syntax:

```
set intfport <1><2><3> auto
```

Example:

```
set intfport 1 auto
```

set intfport ip

Sets an IP address to an interface port.

Syntax:

```
set intfport <1><2><3> ip A.B.C.D E.F.G.H
```

Example:

```
set intfport 1 10.10.10.10 255.255.255.0
```

set intfport speed duplex

Set the speed and duplex setting on the specified interface port.

Syntax:

```
set intfport <1><2><3> speed <10 | 100> duplex <half | full>
```

Parameter	Description
<1> <2> <3>	Enter an interface port ID for which you want to set the speed and duplex.
<10 | 100>	Sets the speed on the interface port. The speed value can be either 10 or 100
<half | full>	Sets the duplex setting on the interface port. Set the value "half' for half duplex and full for 'full' duplex.

Example:

```
set intfport 1 speed 100 duplex full
```

set IPAddressSwap

When you submit samples for analysis through NSP, the source and destination IP information is swapped for the submitted samples. In order to reverse this aberration caused by NSP, McAfee Advanced Threat Defense enables `set IPAddressSwap` command. This command nullifies the swap effect of NSP and displays the correct the source and destination IP information for samples submitted through NSP. However, in case of samples submitted from NGFW to McAfee Advanced Threat Defense the source and destination IP information are displayed correctly. Hence, based on the preference, user can use the following command to enable or disable IPAddressSwap.

Syntax: `set IPAddressSwap <enable><disable>`

By default, set IPAddressSwap is enabled.

Example: `set IPAddressSwap enable`

See also: show IPAddressSwap .

set malware-intfport

Configure the required port to route Internet traffic from an analyzer VM.

ⓘ Before you run this command, make sure that the required port is enabled and configured with an IP address.

Syntax: `set malware-intfport <1><2><3> gateway A.B.C.D`

Example: `set malware-intfport 1 10.10.10.252`

Run the `show intfport 1` and verify the `Malware Interface Port` and `Malware Gateway` entries.

McAfee Advanced Threat Defense uses the configured port to provide Internet access to analyzer VMs. See Internet access to sample files on page 236.

set mgmtport auto

Configures the network port to auto-negotiate the connection between the McAfee Advanced Threat Defense Appliance and the immediate network device.

This command has no parameters.

Syntax:

```
set mgmtport auto
```

Default Value:

By default, the network port is set to **auto** (auto-negotiate).

set mgmtport speed and duplex

Configures the network port to match the speed of the network device connecting to the McAfee Advanced Threat Defense Appliance and to run in full- or half-duplex mode.

Syntax:

```
set mgmtport <speed <10 | 100> duplex <full | half>>
```

Parameter	Description
<10|100>	sets the speed on the Ethernet network port. The speed value can be either 10 or 100 Mbps. To set the speed to 1000 Mbps, use the `set mgmtport auto` command.
<half|full>	sets the duplex setting on the Ethernet network port. Set the value `half` for half duplex and `full` for full duplex.

Default Value:

By default, the network port is set to **auto** (auto-negotiate).

set pdflinks

Use this command to enable or disable validation operation performed by GTI on links embedded inside PDFs, during dynamic analysis.

Syntax: `set pdflinks<enable><disable>`

Sample Output: `set pdflinks enable Enable pdflinks operation`

set filesizes

Enables McAfee Advanced Threat Defense user to change the minimum and maximum file size as per their requirement.

Syntax:

```
set filesizes <type number> <minimum size> <maximum size> <restart engine>
```

Parameter	Description
type number	Type of file submitted for analysis.
minimum size	Minimum file size.
maximum size	Maximum file size.
restart engine	Uses a value of 1 or 0. 1 — Restart AMAS service; this is required for NSP and NGFW integration. 0 — Keeps AMAS service running; use this when submission is through GUI/RestAPI.

The below table describes the different file types and their respective **Type number**, **Minimum File size** and **Maximum File size** :

Type number	File description	Minimum size	Maximum size
1	Windows portable executable (PE) exe, dll or sys file	1024	10000000
2	PDF document file with .pdf extension	2048	25000000
3	Java class data file with .class extension	1024	5000000
4	Microsoft Office older files with .doc, .ppt or .xls extension	5120	10000000
5	Microsfot rich text format file with .rtf extension	1024	10000000
6	Zip file, APK file, or newer Microsoft Office file with .docx, .pptx or .xlsx extension	200	20000000
7	JPEG image file	5120	1000000
8	PNG image file	5120	1000000
9	GIF image/bitmap file	5120	1000000
10	Microsoft DOS executable file with .com extension	1024	5000000
11	Flash file with .swf extension	1024	5000000
12	7-zip compressed archive file with .7z extension	200	10000000
13	RAR compress archive file with .rar extension	200	10000000
14	Microsoft cabinet compressed archive file with .cab and .msi extension	200	10000000
15	Miscellaneous text or script files, for example .js, .bat, .vbs, .xml, .py, .url, .htm etc	100	1000000

For example, if you want to change minimum file size of JPEG image file to 300 bytes then the command `set filesizes 7 300 1000000 0` changes the minimum file size of JPEG image file to 300 bytes.

In case the file size specified by you is beyond the minimum or maximum value listed in the above table, the following error message is displayed:

The <max><min> file size value=<numeric value specified> is invalid

set fips

Enable or disable FIPS mode. This command has no parameters. Restart the McAfee Advanced Threat Defense Appliance when you enable or disable FIPS mode.

Syntax: `set fips <enable> <disable>`

set ftp

When you upload files for analysis using an FTP client or when you import a VMDK file into McAfee Advanced Threat Defense to create an analyzer VM, you use SFTP since FTP is not supported by default. However, if you prefer to use FTP for these tasks, you can enable FTP.

In Common Criteria (CC) mode, FTP is not supported.

Syntax: `set ftp <enable><disable>`

By default, FTP is disabled.

Example: `set ftp enable`

See also: show ftp on page 369.

set headerlog

Use this command to enable or disable the logging of information regarding http header. The *lighttpd* web server is restarted on execution of this command.

This command has no parameters.

Syntax: `set headerlog <enable><disable>`

By default, FTP is disabled.

Example: `set headerlog <enable>`

See also: show headerlog on page 369

set logconfig

Use this command to set the debugging mode to be applied for logs.

Syntax: `set logconfig<enable><disable>`

The following information is displayed using this command:

```
IPS       Enable logconfig support
  AvDat     Disable logconfig support
  CLI
  EPO
  Monitor
  Amaslib
  GTI
  GAM
  MAV
  Scanners
  LB
  DXL
  INI
  SNMP
  CONFIG
```

set heuristic_analysis

See heuristic_analysis on page 353.

set nsp-ssl-channel-encryption

Use this command to configure an encrypted channel for NSP-ATD communication.

Syntax: `set nsp-ssl-channel-encryption <enable><disable>`

Example: `ATD-6000> set nsp-ssl-channel-encryption enable`

Encrypted data transfer from NSP

Use these steps for secure communication between ATD and NSP.

- If encryption is enabled on ATD and NSP, the data sent from NSP to ATD is encrypted and uses an AES128-SHA cipher.
  - Login to Sensor's CLI and enter into debug mode.
  - Execute `set amchannelencryption on`.
  - Login to ATD CLI and execute `set nsp-ssl-channel-encryption enable`.
- If encryption is disabled on ATD and NSP, the data sent from NSP to ATD is not encrypted and uses a NULL-SHA cipher.
  - Login to Sensor's CLI and enter into debug mode.
  - Execute `set amchannelencryption off`.
  - Login to ATD CLI and execute `set nsp-ssl-channel-encryption disable`.

set appliance gateway

Specifies IPv4 address of the gateway for the McAfee Advanced Threat Defense Appliance.

Syntax:

```
set appliance gateway <A.B.C.D>
```

Parameter	Description
<A.B.C.D>	a 32-bit address written as four eight-bit numbers separated by periods. A, B, C or D represents an eight-bit number between 0–255.

Example:

```
set appliance gateway 192.34.2.8
```

set appliance ip

Specifies the McAfee Advanced Threat Defense Appliance IPv4 address and subnet mask. Changing the IP address requires a restart for the changes to take effect. See the `reboot` command for instructions on how to reboot the McAfee Advanced Threat Defense Appliance.

Syntax:

```
set appliance ip <A.B.C.D E.F.G.H>
```

Parameter	Description
<A.B.C.D E.F.G.H>	indicates an IPv4 address followed by a netmask. The netmask strips the host ID from the IP address, leaving only the network ID. Each netmask consists of binary ones (decimal 255) to mask the network ID and binary zeroes (decimal 0) to retain the host ID of the IP address(For example, the default netmask setting for a Class C address is 255.255.255.0).

Example:

```
set appliance ip 192.34.2.8 255.255.0.0
```

set appliance name

Sets the name of the McAfee Advanced Threat Defense Appliance. This name is used to identify the McAfee Advanced Threat Defense Appliance if you integrate it with Network Security Platform.

Syntax:

```
set appliance name <WORD>
```

Parameter	Description
<WORD>	indicates a case-sensitive character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.

Example:

```
set appliance name SanJose_MATD1
```

set stixreportstatus

Use this command to enable or disable the STIX report generation.

This command has no parameters.

Syntax: `set stixreportstatus <enable><disable>`

By default, stixreportstatus is disabled.

Example: `set stixreportstatus <enable>`

See also: show stixreportstatus on page 372

set tcpdump

Use this command to set packet capture functionality.

Syntax: `set tcpdump`

```
set tcpdump<start><port options seepearted by underscore>
```

Example: `set tcpdump start -i_eth0_-c_10`

```
set tcpdump<stop>
```

Parameter	Description
start	Starts the packet capture operation on the specified tcp dump
stop	Stops the packet capture operation

set uilog

Use this command to set the amount of UI access information to be logged. Level varies from 1 to 7.

Syntax:

```
set uilog<seconds>
```

Parameter	Description
<numeric>	Sets the amount of UI access information to be logged.

```
ATD-6000> set uilog 5

 new log level is 5
```

set ui-timeout

Specifies the number of minutes of inactivity that can pass before the McAfee Advanced Threat Defense web application connection times out.

Syntax:

```
set ui-timeout <60 - 86400>
```

Parameter	Description
<60 - 86400>	You can set a timeout period from 60 to 86400 seconds.

Example: `set ui-timeout 600`

Default Value: 15 minutes

set whitelist

Use this command to configure checking of whitelist by McAfee Advanced Threat Defense.

Syntax: `set whitelist <enable><disable>`

Example: `set whitelist enable`

show

Shows all the current configuration settings on the McAfee Advanced Threat Defense Appliance.

This command has no parameters.

Syntax:

```
show
```

Information displayed by the `show` command includes:

[Sensor Info]

- System Name
- Date
- System Uptime
- System Type
- Serial Number
- Software Version
- Active Version
- Backup Version
- MGMT Ethernet Port

[Sensor Network Config]

- IP Address
- Netmask
- Default Gateway
- DNS address

show dat version

Use this command to see the current DAT version of analyzing options.

Syntax: `show dat version`

Sample Output:

```
AV  DAT    version=7868
AV  Engine version=5700
GAM DAT    version=3811
GAM Engine version=7001.1302.1842
```

show ds status

Use this command to see status of all analyzing options.

Syntax: `show ds status`

This command has no parameters.

Sample Ouptut:

```
GTI is alive

MAV is alive

GAM is alive

Yara is alive
```

show epo-stats nsp

Displays the count of requests sent to McAfee ePO, the count of responses received from McAfee ePO, and the count of requests that failed.

Syntax: `show epo-stats nsp`

This command has no parameters.

show filequeue

Displays the file queue statistics like the estimated average processing time, analyzing time, files in waiting and so on.

This command has no parameter.

Syntax:`show filequeue`

Following is the information displayed by the `show filequeue` command:

```
Processing  Time:    58.00
Analyzing   Time:    58.00
Files in waiting: 0
files in SandBox: 0
Estimated average processing time for all samples:    58.00 seconds
```

show filesizes

Displays all the filetypes supported by McAfee Advanced Threat Defense with details such as type number, minimum and maximum file size in bytes, and short description.

This command has no parameters.

Syntax:

`show filesizes`

Following is the information displayed by the `show filesizes` command:

Type number	File description	Minimum size	Maximum size
1	Windows portable executable (PE) file, PE+ file, dll and sys file	1024	10000000
2	PDF document file with .pdf extension	2048	25000000
3	Java class data file with .class extension	1024	5000000
4	Microsoft Office older files with .doc, .ppt or .xls extension	5120	10000000
5	Microsfot rich text format file with .rtf extension	1024	10000000
6	Zip file, APK file, or newer Microsoft Office file with .docx, .pptx or .xlsx extension	200	20000000
7	JPEG image file	5120	1000000
8	PNG image file	5120	1000000
9	GIF image/bitmap file	5120	1000000
10	Microsoft DOS executable file with .com extension	1024	5000000
11	Flash file with .swf extension	1024	5000000
12	7-zip compressed archive file with .7z extension	200	10000000
13	RAR compress archive file with .rar extension	200	10000000
14	Microsoft cabinet compressed archive file with .cab and .msi extension	200	10000000
15	Miscellaneous text or script files, for example .js, .bat, .vbs, .xml, .py, .url, .htm etc	100	1000000

show fips

Shows if FIPS is enabled or disabled currently. This command has no parameters.

Syntax: `show fips`

show ftp

Use this command to know if FTP is enabled or disabled currently. By default, FTP is disabled.

Syntax: `show ftp`

See also: set ftp on page 363.

show headerlog

This command shows the current status of the http header log.

This command has no parameters.

Syntax: `show headerlog`

Sample Output: `Header log is disable`

show history

Displays the list of CLI commands issued in this session.

Syntax: `show history`

This command has no parameters.

show heuristic_analysis

See heuristic_analysis on page 353.

show intfport

Shows the status of the specified interface port or the management port of McAfee Advanced Threat Defense.

Syntax: `show intfport <mgmt><1><2><3>`

Information displayed by the `show intfport` command includes:

- Whether the port's administrative status is enabled or disabled.
- The port's link status.
- The speed of the port.
- Whether the port is set to half or full duplex.
- Total packets received.
- Total packets sent.
- Total CRC errors received.
- Total other errors received.

- Total CRC errors sent.
- Total other errors sent.
- IP address of the port.
- MAC address of the port.
- Whether the port is used to provide Internet access to analyzer VMs.
- If configured to provide Internet access to analzyer VMs, then the corresponding gateway for this traffic.

show logconfig

Use this command to list the current debug mode employed for debugging.

Syntax: `show logconfig`

This command has no parameters.

Sample Output: `Logging is ON, mode: send to syslog`

show pdflinks

Use this command to view whether or not validation operation is performed by GTI on links embedded inside PDFs, during dynamic analysis.

Syntax: `show pdflinks`

This command has no parameters.

Sample Output: `GTI validation of PDF URLs is OFF`

set IPAddressSwap

When you submit samples for analysis through NSP, the source and destination IP information is swapped for the submitted samples. In order to reverse this aberration caused by NSP, McAfee Advanced Threat Defense enables `set IPAddressSwap` command. This command nullifies the swap effect of NSP and displays the correct the source and destination IP information for samples submitted through NSP. However, in case of samples submitted from NGFW to McAfee Advanced Threat Defense the source and destination IP information are displayed correctly. Hence, based on the preference, user can use the following command to enable or disable IPAddressSwap.

Syntax: `set IPAddressSwap <enable><disable>`

By default, set IPAddressSwap is enabled.

Example: `set IPAddressSwap enable`

See also: show IPAddressSwap .

show msu

Displays all the msu files copied to Advanced Threat Defense via SFTP.

Syntax: `show msu`

show nsp scandetails

Shows the file scan details regarding the integrated IPS Sensors.

Syntax: `show nsp scandetails <Sensor IP address>`

If you do not specify the Sensor IP address, the details are displayed for all the Sensors integrated with the McAfee Advanced Threat Defense Appliance.

Information displayed by the `show nsp scandetails` command includes:

- The IP address of the IPS Sensor.
- Total number of packets received from the Sensor.
- Total number of packets sent to the Sensor.
- The timestamp of when the last packet was sent to and received from the Sensor.
- The encryption method used for the communication with the Sensor.
- Session handle null counts.
- Count of internal errors.
- Count of unknown commands received from the Sensor.
- File string null.
- File data null.
- Count of unknown files.
- Count of out of order packets.
- Count of MD5 mismatches between what was sent by the Sensor and what was calculated by McAfee Advanced Threat Defense.
- Count of memory allocation failures.
- File transfer timeout.
- New file count.
- Count of shared memory allocation failures.
- Count of the number of static analysis responses sent.
- Count of the number of dynamic analysis responses sent.
- Count of scan request received.
- MD5 of the last file that was streamed by the Sensor.

show route

This command is used to show routes that you configured using the `route add` command as well as the system IP routing table.

Syntax:

```
show route
```

The details from a sample output of the command in the following table.

Table 10-2 System IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.10.10.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
11.11.11.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
12.12.0.0	0.0.0.0	255.255.0.0	U	0	0	0	mgmt
13.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	mgmt
0.0.0.0	10.10.10.253	0.0.0.0	UG	0	0	0	mgmt

show stixreportstatus

This command shows the current status of the stixreportstatus.

This command has no parameter.

Syntax: `show stixreportstatus`

Sample Output: `STIX reporting is OFF`

show tcpdump

Use this command to display the current status of packet capture functionality. The maximum file size for the capture is 10MB.

Syntax: `show tcpdump`

This command has no parameters.

Sample Output: `TCPdump is not running`

show ui-timeout

Displays the McAfee Advanced Threat Defense web application client timeout in seconds.

Syntax: `show ui-timeout`

Sample output: `Current timeout value: 600`

show uilog

Use this command to check the current level of uilog.

This command has no parameters.

Syntax:

```
show uilog
```

Following is the information displayed by the `show uilog` command:

```
ATD-6000> show uilog
Current log level is 7
```

show version

Displays zebra version of McAfee Advanced Threat Defense.

This command has no parameters.

Syntax:

```
show version
```

Following is the information displayed by the `show version` command:

```
Zebra 0.95a ().
Copyright 1996-2004, Kunihiro Ishiguro.
ATD-3000>
```

show waittime

Displays wait time threshold set for McAfee Email Gateway.

Syntax: `show waittime`

Sample output: `Current MEG wait time threshold=780 seconds`

shutdown

Halts the McAfee Advanced Threat Defense Appliance so you can power it down. Then, after about a minute, you can power down the McAfee Advanced Threat Defense Appliance **manually** and unplug both the power supplies. McAfee Advanced Threat Defense Appliance does not power off automatically. You must confirm that you want to shut it down.

This command has no parameters.

Syntax:

```
shutdown
```

status

Shows McAfee Advanced Threat Defense system status, such as the health and the number of files submitted to various engines.

This command has no parameters.

Syntax: `status`

Sample output:

```
System Health Status : good

Sample files received count: 300

Sample files submitted count: 300

GTI Scanner files submitted count: 50

GAM Scanner files submitted count: 100

MAV Scanner files submitted count: 200

Sandbox files submitted count: 25

Sandbox files finished count: 25

Sample files finished count: 300

Sample files error count: 0
```

terminal

Set the number of lines for display on the screen of McAfee Advanced Threat Defense

Syntax:

```
terminal <length>¦no
```

Parameter	Description
<length>	Sets the number of lines for display on the screen. The value ranges from 0 - 512.
no	Negates the previous command or sets the default value.

update_avdat

By default, McAfee Advanced Threat Defense updates the DAT files for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. To update these files immediately, use the `update_avdat` command.

This command has no parameters.

Syntax: `update_avdat`

vmlist

Displays list of all the VMs configured on the McAfee Advanced Threat Defense

Syntax: `vmlist`

watchdog

The watchdog process reboots the McAfee Advanced Threat Defense Appliance whenever an unrecoverable failure is detected.

Syntax:

```
watchdog <on | off | status>
```

Parameter	Description
<on>	Enables the watchdog.
<off>	Disables the watchdog. Use it if the Appliance reboots continuously due to repeated system failure.
<status>	Displays the status of the watchdog process.

set malware-intfport mgmt

By default, Internet access to analyzer VMs is through the McAfee Advanced Threat Defense's management port (eth-0). Use this command, if you had configured a different port for routing Internet traffic and want to revert to the management port.

Syntax: `set malware-intfport mgmt`

Run the `show intfport mgmt` and verify the `Malware Interface Port` and `Malware Gateway` entries.

McAfee Advanced Threat Defense uses the management port to provide Internet access to analyzer VMs. See Internet access to sample files on page 236.

whitelist

Use the following commands to manage the whitelist of McAfee Advanced Threat Defense.

Syntax:

- To add an MD5 to the whitelist, use `whitelist add <md5>`

  Example: `whitelist add 254A40A56A6E68636E1465AF7C42B71F`

- To delete an MD5 from the whitelist, use `whitelist delete <md5>`

  Example: `whitelist delete 254A40A56A6E28836E1465AF7C42B71F`

- To check if an MD5 is present in the whitelist, use `whitelist query <md5>`

  Example: `whitelist query 254A40A56A6E28636E1465AF7C42B71F`

- To check the status if checking the whitelist status is currently enabled, use `whiteliststatus`

Index